Model Tribal Data Sharing Agreement

The American Indian Health Commission Model Data Sharing Agreement (DSA) provides example terms and conditions under which (1) a Tribal jurisdiction is provided informed consent on how Tribal data, including sensitive communicable disease data about their Tribe and their Tribal members, are used or shared with third parties; and (2) a Tribal jurisdiction is treated as a sovereign government with equitable access to public health data to protect the health and safety of their community members. Tribal data sharing agreements should be developed in consultation with Tribal governments. The American Indian Health Commission (AIHC) will continue to update this document here as we receive additional input from Tribes. Please send any feedback to AIHC.general.delivery@outlook.com.

The AIHC adapted this DSA from a standard Washington State Department of Health Data Sharing Agreement. Changes made to any Washington State Department of Health Data Sharing Agreements in this DSA are endorsed solely by the AIHC and not the Washington State Department of Health.

A special thanks. *This DSA is the result of the collaborative efforts of many individuals including Tribal staff, public health leadership, public health policy experts, epidemiologists, and attorneys. We wish to acknowledge and thank those who contributed their knowledge, expertise, and most importantly, their time, to ensuring Tribes have equitable access to the data necessary to protect and improve the health of their people.*

First Published: 7-31-23
Last Updated: 8-23-23

Table of Contents

TRIBAL DATA SHARING AGREEMENT (TDSA)
BETWEEN
[NAME OF STATE AGENCY]
AND
[NAME OF TRIBAL JURISDICTION]

This Data Sharing Agreement ("Agreement" or DSA) is made and entered into by **[NAME OF STATE AGENCY]** and the **[NAME OF TRIBAL JURISDICTION]**. This agreement does not confer any remedies or rights upon any person or entity other than the signatories.

1. PURPOSE

This Agreement establishes the terms and conditions under which:

a. the **[NAME OF TRIBAL JURISDICTION]** and **[NAME OF STATE AGENCY]** collect, manage, use, disclose, and safeguard Tribal and American Indian and Alaska Native information and data; and

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

2. DEFINITIONS

a. American Indian/Alaska Native population data means de-identified, aggregate, public or private data or information on or about American Indian or Alaska Native people that does not identify individual Tribes or Tribal membership.

b. Authorized user means a recipient's employees, agents, assignees, representatives, independent contractors, or other persons or entities authorized by the data recipient to access, use, or disclose information through this agreement.

c. 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.

d. Breach of security means an action (either intentional or unintentional) that bypasses security controls or violates security policies, practices, or procedures.

e. Case and contact investigation system means an electronic data system used for disease case and contact investigation and data collection.

f. Confidential information means data or information that is protected from public disclosure under **[INSERT APPLICABLE FEDERAL OR STATE STATUTE]**.

g. Data means facts or items of information. Data may also include quantitative and/or qualitative data. Quantitative data is measurable, often used for comparisons, and involves counting of people, behaviors, conditions, or other discrete events. Qualitative data is a broad category of data that can include almost any non-numerical data that can be observed but not measured.

h. Data storage means electronic, magnetic, optical, or mechanical media that records and preserves data and/or information.

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

j. Direct identifier means direct identifiers in research data or records including names; postal address data (other than town or city, state and zip code); telephone numbers, fax numbers, e-mail addresses; social security numbers; medical record numbers; health plan beneficiary numbers; account numbers; birth certificates, certificate /license numbers; vehicle identifiers and serial numbers, including license plant numbers; device identifiers and serial numbers; web universal resource locators (URLs); internet protocol (IP) address numbers; biometric identifiers, including finger and voice prints; and full face photographic images and any comparable images.

k. 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.

l. 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.

m. Electronic Surveillance System for the Early Notification of Community-based Epidemics or ESSENCE means the Centers for Disease Control (CDC) National Syndromic Surveillance Program (NSSP) platform which authorized users access through a web browser interface. ESSENCE contains syndromic surveillance data from **[INSERT STATE]** and other participating states and includes analytical tools with which authorized users may interact with the data.

n. 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.

o. Human subjects research 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.

p. Identifiable data or records means data or records that contain 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.

q. Immunization data means data entered into or retrieved from the **[NAME OF STATE AGENCY]** Immunization Information System **[INSERT ACRONYM]**.

r. **[NAME OF STATE AGENCY]** immunization information system means **[NAME OF STATE AGENCY]** lifetime registry that keeps track of immunization records for people of all ages in **[NAME OF STATE AGENCY]**. The system is a secure, web-based tool for healthcare providers and schools. The **[NAME OF STATE AGENCY]** Immunization Information System

connects people who receive, administer, record, and order vaccines in **[NAME OF STATE AGENCY]**.

s. Indirect identifier in research data or records means a single data element that on its own does not identify an individual person, but when combined with other indirect identifiers can be used to identify an individual person. Examples of indirect identifiers include, but are not limited to race, ethnicity, Tribe of membership, Tribe of affiliation, Tribal census tract, occupation, industry and employer. Other indirect identifiers according to HIPAA Safe Harbor include all geographic identifiers smaller than a state, including street address, city, county, precinct, zip code, and their equivalent postal codes, except for the initial three digits of a ZIP code; all elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 74 and all elements of dates (including year) indicative of such age, except that such age and elements may be aggregated into a single category of age 75 or older.

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

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

v. Linked data includes data obtained from more than one data system as a result of matching to identify the same person or persons within each data system. Matching may be done using computer algorithms or manual review.

w. **[NAME OF NOTIFIABLE DISEASE REPORTING SYSTEM]** is the **[NAME OF STATE AGENCY]**'s electronic disease surveillance system for notifiable conditions per **[INSERT STATE LAW OR REGULATION]** that allows public health staff in **[NAME OF STATE AGENCY]** to receive, enter, manage, process, track and analyze disease-related data. **[NAME OF NOTIFIABLE DISEASE REPORTING SYSTEM]** allows secure communication and coordination among Tribal, state, and local health departments.

x. Potentially Identifiable Information means data containing variables other than name and address that can still be potentially identifiable if indirect identification of an individual or organization is possible.

y. Restricted confidential information means confidential information where especially strict handling requirements are dictated by statutes, rules, regulations or contractual agreements, unauthorized disclosure of which may result in enhanced legal sanctions.

z. Statewide data system operated by the **[NAME OF STATE AGENCY]** means a data system that **[NAME OF STATE AGENCY]** operates and controls for the benefit and use of all local and Tribal jurisdictions.

aa. 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.

bb. Tribal Data means public or private data or information on or about a Tribe or its people subject to Tribal rights of ownership and control. This 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. For the purpose of this agreement, Tribal data means either:

i. data or information that is specific to an individual Tribe; or

ii. data or information that is specific to more than one Tribe but does not identify individual Tribe(s).

cc. Tribal data sovereignty means the inherent legal authority of Tribes to administer the collection, ownership, application and interpretation of Tribal data or information even if it is collected by federal, state, or local governments.

dd. Tribe as defined under Section 4 of the Indian Health Care Improvement Act (codified at 25 U.S.C 1603(14) 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.

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

a. Tribes are Public Health Authorities. In implementing this Agreement, **[NAME OF STATE AGENCY]**, shall honor and treat Tribes as both health jurisdictions and public health authorities as recognized under 45 CFR § 164.501.

b. Tribes are Public Health Jurisdictions. In implementing this Agreement, **[NAME OF STATE AGENCY]** shall honor and treat Tribes as public health jurisdictions with all the public health powers that exceed those of non-governmental public health authorities. Tribes possess all attendant rights and powers of governments to protect the health and welfare of their citizens as recognized by Worcester v. Georgia, 31 U.S. (6 Pet.) 515, 559 (1832); See also, Cherokee Nation v. Georgia, 30 U.S. (5 Pet.) 1 at 16 (1831). This governmental authority includes, but is not limited to, the power to conduct isolation and quarantine, perform case and contact investigations, dispense, and distribute vaccines, close off reservation borders to protect Tribal citizens, conduct data surveillance, and protect the use of their nation's public health data by outside entities. Such power may not be divested or diminished by a state government or any other party, and no federal law has divested Tribes of their public health authority.

4. OWNERSHIP OF 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. The **[NAME OF TRIBAL JURISDICTION]** and **[NAME OF STATE AGENCY]** shall have joint ownership in data and information in **[NAME OF STATE AGENCY]** data systems regarding the Tribe, its Tribal citizens, and persons who reside within the Tribe's jurisdiction, under this Agreement;

b. This agreement shall not limit the **[NAME OF TRIBAL JURISDICTION]**'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 the **[NAME OF STATE AGENCY]** collects, manages, uses, discloses, and safeguards **[NAME OF TRIBAL JURISDICTION]**'s data.

a. When informed consent is required. **[NAME OF STATE AGENCY]** must obtain prior express written consent using the Tribal Nation Data Use Form (Appendix E) from the **[NAME OF TRIBAL JURISDICTION]** under the following conditions:

i. Prior to **[NAME OF STATE AGENCY]** publishing data/information that **[NAME OF STATE AGENCY]** knows or has reason to know are **[NAME OF TRIBAL JURISDICTION]**'s data or information in a manner that allows those data to be identified as this 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;

ii. Prior to sharing data/information that **[NAME OF STATE AGENCY]** knows or has reason to know are [NAME OF TRIBAL JURISDICTION]'s data or information with a third party as defined under Section 2(aa) unless the **[NAME OF STATE AGENCY]** receives a release of data and/or information (ROI) executed by the **[NAME OF TRIBAL JURISDICTION]**. This subsection 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. **[NAME OF STATE AGENCY]** shall discontinue any current access to individual or multiple datasets through linked data that contains the **[NAME OF TRIBAL JURISDICTION]**'s data unless the third party has an ROI in accordance with Section 5(a)(ii). The ROI shall contain the following:

(1) Who is authorizing the release;

(2) Why the information is being disclosed;

(3) A list of each individual **[NAME OF STATE AGENCY]** dataset a third-party is seeking access to;

(4) The cut-off date for the ROI. The cut-off date for an ROI shall not exceed one year;

(5) Requirements for use of linkages; and

(6) Requirements for data disposition, security, confidentiality, storage, and human subjects research limitations.

iii. Prior to researching [NAME OF TRIBAL JURISDICTION]'s data or information in a manner that includes Tribal membership or association or can uniquely identify **[NAME OF TRIBAL JURISDICTION]**; and

iv. Prior to analyzing [NAME OF TRIBAL JURISDICTION]'s data or information in a manner that includes Tribal membership or association or can uniquely identify the **[NAME OF TRIBAL JURISDICTION]**.

b. Updating existing agreements. **[NAME OF STATE AGENCY]** will update all data sharing agreements with third parties to reflect the requirements of this section.

c. Timelines for submitting Tribal Nation data use form. The Tribe will respond no later than 60 days after receipt of the Tribal Nation Data Use Form. If the Tribe does not respond within 60 days of receiving **[NAME OF STATE AGENCY]**'s request, the **[NAME OF STATE AGENCY]** request will be deemed approved. **[NAME OF STATE AGENCY]** can request approval prior to 60 days by providing justification for an expedited process.

d. Prohibited collection of data. Unless otherwise agreed to by the Tribe in the Tribal Nation Data Use Form (Appendix E), **[NAME OF STATE AGENCY]** will not collect Tribe of membership or Tribal affiliation, or Tribal Census Tract identification in any **[NAME OF STATE AGENCY]** dataset.

e. Exceptions. This section provides exceptions for when **[NAME OF STATE AGENCY]** shall not be required to seek prior express written permission under Section 5. Unless otherwise stated, **[NAME OF STATE AGENCY]** shall still be required to provide notification to the **[NAME OF TRIBAL JURISDICTION]** utilizing the Tribal Nation Data Use Form (Appendix E) as soon as **[NAME OF STATE AGENCY]** has reason to know whether the data or information involves Tribal data or information. The exceptions include the following:

i. A request under the **[INSERT STATE PUBLIC RECORDS LAW]**. The **[INSERT STATE PUBLIC RECORDS LAW]** requires release of the data or information with a minimum of **[INSERT NUMBER OF DAYS]** notice as per **[NAME OF STATE AGENCY]** Public Records Policy and Procedure;

ii. A state or federal statute or regulation that prohibits or limits **[NAME OF STATE AGENCY]** compliance with Section 5;

iii. Compulsory legal process, court order, or a settlement or a consent decree which prohibits or limits **[NAME OF STATE AGENCY]** compliance with Section 5;

iv. An existing contract, cooperative agreement or grant prohibits or limits **[NAME OF STATE AGENCY]** compliance with Section 5. This subsection is subject to Section 5(b) which requires **[NAME OF STATE AGENCY]** to update all data sharing agreements with third parties to reflect the requirements of this section and discontinue future use of data under this Agreement in a manner that violates Section 5(a)(ii);

v. Sharing with a state agency, federal agency, local health jurisdiction, or Tribe when **[NAME OF STATE AGENCY]** 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 **[INSERT APPLICABLE STATE COMMUNICABLE DISEASE REGULATION OR STATUTE]** within that agency's jurisdiction, a local health jurisdiction, or Tribal jurisdiction in alignment with current public health Tribal/local/state practice;

vi. Data reports and data visualizations published prior to execution of this Agreement. No Tribal Nation Data Use Form is required. This subsection shall not include updates to prior reports and data visualizations after execution of this Agreement;

vii. Data analyses that are conducted to understand and correct data reporting interruptions or problems;

viii. Data analyses undertaken to address data quality concerns, such as to identify invalid data, missing or incomplete data; and

ix. Whenever an individual is requesting **[NAME OF STATE AGENCY]** information or records that relate to them or the provision of health care services to them. No Tribal Nation Data Use Form is required.

6. ACCESS TO STATE AGENCY DATASETS/DATABASES

a. Current database/dataset access. Access to the following **[NAME OF STATE AGENCY]** data by **[NAME OF TRIBAL JURISDICTION]**, including upgraded systems to those datasets, is provided for the purposes outlined in Section 1 of this Agreement (Access to checked boxes only. If necessary, attach exhibit with additional requirements specific to dataset):

Name of Database		Description	Read/Write Access	Exhibit #
☐		Statewide notifiable disease reporting system	Both	
☐		Linked Immunization Administration Data in state notifiable disease reporting system		
☐		Linked Death Data in state notifiable disease reporting system		
☐		Linked syndromic surveillance data in state notifiable disease reporting system		
☐		Linked case and contact investigation data in state notifiable disease reporting system		
☐		State case and contact investigation system (case and contact investigation data)		
☐		State Immunization Information System		

b. Future dataset/database access. **[NAME OF TRIBAL JURISDICTION]** can choose to request access to additional **[NAME OF STATE AGENCY]** 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 **[NAME OF TRIBAL JURISDICTION]** who have signed the Statement of Confidentiality document set forth in Appendix A. These entities meet the definition of 'government agencies' **[INSERT NAME OF STATE STAUTE OR REGULATION]**.

8. USE OF DATA AND INFORMATION

a. This Agreement does not prevent **[NAME OF TRIBAL JURISDICTION]** from conducting human subjects research, provided there is approval through official Tribal process, which may include approval by Tribal council, the 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. Tribal program staff cannot give approval to start human subjects research.

b. Data reporting must align with **[NAME OF STATE AGENCY]**'s Small Numbers Guidelines (Appendix D).

9. CONFIDENTIALITY

[NAME OF STATE AGENCY] and **[NAME OF TRIBAL JURISDICTION]** agree to:

a. Follow **[NAME OF STATE AGENCY]** small numbers guidelines as well as dataset specific small numbers requirements. (Appendix D)

b. Limit access and use of the data/information:

   i. To the minimum amount of data/information;

   ii. To the fewest people; and

   iii. For the least amount of time required to do the work.

c. Ensure that all people with access to the data/information understand their responsibilities regarding it.

d. Ensure that every person (e.g., employee or agent) with access to the information signs and dates the "Statement of Confidentiality Form" (Appendix A) before accessing the information.

e. Retain a copy of the signed and dated "Statement of Confidentiality 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

The **[NAME OF TRIBAL JURISDICTION]** assures that its security practices and safeguards meet **[INSERT APPLICABLE STATE DATA SECURITY STANDARD]**.

For the purposes of this Agreement, compliance with the HIPAA Security Standard and all subsequent updates meets **[INSERT APPLICABLE STATE DATA SECURITY STANDARD]** "Securing Information Technology Assets."

The **[NAME OF TRIBAL JURISDICTION]** agrees to adhere to the Data Security Requirements in Appendix B and this data sharing agreement. The **[NAME OF TRIBAL JURISDICTION]** 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

[NAME OF TRIBAL JURISDICTION], 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 **[NAME OF STATE AGENCY]** Business Contact.

13. BREACH NOTIFICATION

The **[NAME OF TRIBAL JURISDICTION]** shall notify the **[NAME OF STATE AGENCY]** Chief Information Security Officer at **[INSERT EMAIL ADDRESS]** within ten (10) business days of any suspected or actual breach of security or confidentiality of information covered by the Agreement.

The **[NAME OF STATE AGENCY]** Chief Information Security Officer shall notify the **[NAME OF TRIBAL JURISDICTION]** at **[INSERT EMAIL ADDRESS]** within ten (10) business days of any suspected or actual breach of security or confidentiality of information pertaining to Tribal data/information or American Indian/Alaska Native data/information covered by the Agreement.

14. RE-DISCLOSURE OF DATA/INFORMATION

a. 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 the law requires or as this Agreement permits.

b. If **[NAME OF STATE AGENCY]** 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, the **[NAME OF STATE AGENCY]** will notify the **[NAME OF TRIBAL JURISDICTION]** who is the subject of the data/information of the request no less than ten (10) business days prior to disclosing to the requestor.

c. Notice pursuant to this section must:

    i. Be in writing;

    ii. Include a copy of the request or some other writing that shows the:

        (1) Date the party received the request; and

(2) The **[NAME OF STATE AGENCY]** records that the party believes are responsive to the request and the identity of the requestor, if known.

15. ATTRIBUTION REGARDING DATA/INFORMATION

[NAME OF TRIBAL JURISDICTION] and **[NAME OF STATE AGENCY]** agree to cite their organizational name as the source of interpretations, calculations, or manipulations of the data/information subject of this Agreement.

16. STATUTORY AUTHORITY TO SHARE DATA/INFORMATION

[NAME OF STATE AGENCY] statutory authority to obtain and disclose the confidential information or limited Dataset(s) identified in this Agreement to health jurisdictions/governmental departments:

[LIST APPLICABLE STATE STATUTES AND REGULATIONS]

17. COMPLIANCE WITH DSA

a. **[NAME OF STATE AGENCY]** will establish written Tribal data sharing policies and procedures that implement the requirements under this Agreement.

b. **[NAME OF STATE AGENCY]** will provide regular staff orientations and training on the policies and procedures referenced in subsection (a) under this section. Orientations and training shall include the education and information on protecting Tribal and AI/AN Population Data and Information and the Tribal Nation Data Use Form.

c. **[NAME OF STATE AGENCY]** will work to ensure staff compliance with Tribal data sharing policies and address any violations in accordance with the **[NAME OF STATE AGENCY]** Tribal data sharing policies and procedures and **[NAME OF STATE AGENCY]** human resources policies and procedures.

18. AGREEMENT ALTERATIONS AND AMENDMENTS

This Agreement including all Exhibits and Appendices 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.

19. CAUSE FOR IMMEDIATE TERMINATION

The **[NAME OF TRIBAL JURISDICTION]** and **[NAME OF STATE AGENCY]** acknowledge that unauthorized use or disclosure of the data/information or use of data inconsistent with this data sharing agreement and appendices may result in the immediate termination of this Agreement.

20. CONFLICT OF INTEREST

a. The **[NAME OF STATE AGENCY]** may, by written notice to the **[NAME OF TRIBAL JURISDICTION]**, terminate the right of the **[NAME OF TRIBAL JURISDICTION]** to proceed under this Agreement if it is found, after due notice and examination by the Contracting Office that gratuities in the form of entertainment, gifts or otherwise were offered or given by the **[NAME OF TRIBAL JURISDICTION]**, or an agency or representative of the **[NAME OF TRIBAL JURISDICTION]**, to any officer or employee of the **[NAME OF STATE AGENCY]**, 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.

b. In the event this Agreement is terminated as provided in (a) above, the **[NAME OF STATE AGENCY]** shall be entitled to pursue the same remedies against the **[NAME OF TRIBAL JURISDICTION]** as it could pursue in the event of a breach of the Agreement by the **[NAME OF TRIBAL JURISDICTION]** The rights and remedies of the **[NAME OF STATE AGENCY]** provided for in this section are in addition to any other rights and remedies provided by law. Any determination made by the Contracting Office under this clause shall be an issue and may be reviewed as provided in the "disputes" clause of this Agreement.

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 **[NAME OF STATE AGENCY]** 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. DISPUTES

Except as otherwise provided in this Agreement, when a genuine dispute arises between the **[NAME OF STATE AGENCY]** and the **[NAME OF TRIBAL JURISDICTION]** and it cannot be resolved, either party may submit a request for a dispute resolution to the **[NAME OF STATE AGENCY]** Contracts and Procurement Unit. The parties agree that this resolution process shall precede any action in a judicial and quasi-judicial tribunal. A party's request for a dispute resolution must:

a. Be in writing and state the disputed issues, and

b. State the relative positions of the parties, and

c. State the **[NAME OF TRIBAL JURISDICTION]** name, address, and his/her department agreement number, and

d. Be mailed to the **[NAME OF STATE AGENCY]** contracts and procurement unit, **[INSERT ADDRESS]** within thirty (30) calendar days after the party could reasonably be expected to have knowledge of the issue which he/she now disputes.

This section is subject to Section 32 of this Agreement and does not diminish any rights or protections afforded 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 BUSINESS DATA/INFORMATION NOT OTHERWISE PROTECTED BY LAW AND UNRELATED TO CONTRACT WORK

During the course of this contract, the **[NAME OF TRIBAL JURISDICTION]** may inadvertently become aware of data/information unrelated to this agreement. **[NAME OF TRIBAL JURISDICTION]** will treat such data/information respectfully, recognizing **[NAME OF STATE AGENCY]** 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. CONTACT INFORMATION FOR PARTIES TO THE AGREEMENT

TRIBE	STATE AGENCY
Tribe	**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:**

25. CHOICE OF LAW

This Agreement is entered into pursuant to and under the authority granted by the laws of the state of **[NAME OF STATE]**, **[INSERT TRIBE]**, 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:

a. Federal statutes and rules, to the extent applicable;

b. Applicable **[NAME OF STATE]** state and statutes and rules;

c. **[NAME OF TRIBAL JURISDICTION]** laws, to the extent applicable; and

d. 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. **[NAME OF STATE AGENCY]** and the **[NAME OF TRIBAL JURISDICTION]** shall cooperate in the defense of tort lawsuits, when possible and subject to Section 32 of this Agreement.

27. LIMITATION OF AUTHORITY

Only the Authorized Signatory for **[NAME OF STATE AGENCY]** 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 **[NAME OF STATE AGENCY]**. 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 **[NAME OF STATE AGENCY]**.

28. 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.

29. 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.

30. TERMINATION

Either party may terminate this Agreement upon 30 days prior written notification to the other party. If this Agreement is so terminated, the parties shall be liable only for performance rendered or costs incurred in accordance with the terms of this Agreement prior to the effective date of termination.

31. WAIVER OF DEFAULT

This Agreement, or any term or condition, may be modified only by a written amendment signed by both parties. Either party may propose an amendment.

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

32. SOVEREIGN IMMUNITY

Nothing in this Agreement or attached exhibits and/or appendices shall constitute a waiver of federal or Tribal sovereign immunity.

33. ENTIRE AGREEMENT

a. This Agreement and attached Exhibit(s) and Appendices contain all the terms and conditions agreed upon by the parties with the exception that additional Exhibits may be incorporated into this Agreement in accordance with Section 6(b) of this Agreement.

b. This Agreement supersedes all prior conversations, proposals, negotiations, understandings and contracts/agreements, whether written or oral unless otherwise agreed to in writing by the parties.

34. TERM OF AGREEMENT AND EFFECTIVE DATE

All provisions of this Agreement will be effective on the date of execution. The term of this agreement shall be seven 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.

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

_____ _____

[NAME OF STATE AGENCY] /TITLE **[NAME OF TRIBAL JURISDICTION]/TITLE**

_____	_____
Signature	Signature

APPENDIX A: STATEMENT OF CONFIDENTIALITY AND TRIBAL DATA PROTECTION FORM

Confidential information and Tribal data as defined under section 2 of the Agreement are protected from disclosure by federal, state law, or in the Agreement. Examples of confidential information are:

- Healthcare information that is identifiable to a specific person under **[INSERT STATE PRIVACY LAW/REGULATION]**, and residential / personal contact information of public employees, social security numbers, and financial account numbers under **[INSERT STATE PRIVACY LAW/REGULATION]**.
- Infrastructure and technology system artifacts (such as asset inventories, IP addressing schemes, routing tables, network devices, event logs, operating systems, server names, architectural network/system diagrams)
- Tribal Data means public or private data or information on or about a Tribe or its people subject to Tribal rights of ownership and control. This 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. For purposes of this agreement, Tribal data means (1) data or information that is specific to an individual Tribe; or (2) data or information that is specific to more than one Tribe but does not identify individual Tribe(s).

RESPONSIBILITIES REGARDING CONFIDENTIAL INFORMATION

I understand it is my responsibility to maintain the confidentiality of certain data and information, including Tribal data/information, that I may access, use or otherwise acquire from **[NAME OF STATE AGENCY]**. I understand I am responsible for knowing what information is confidential. If in doubt I will work with the **[NAME OF STATE AGENCY]** contact or the **[NAME OF STATE AGENCY]** Privacy Officer to determine if the information I access, use, or otherwise acquire is confidential.

I will not at any time, or in any manner, either directly or indirectly, discuss, release, or otherwise disclose **[NAME OF STATE AGENCY]** confidential data and information to anyone outside the scope of my work, except as authorized by law.

I understand that **[NAME OF STATE AGENCY]** may monitor, audit, or investigate use of the confidential information I access, use, or otherwise acquire through this engagement. Monitoring, auditing, or investigating includes, but is not limited to, "salting" by **[NAME OF STATE AGENCY]**. Salting is the act of placing a record containing unique but false information in a database that can be used later to identify inappropriate disclosure of information.

PENALITES FOR DISCLOSING CONFIDENTIAL INFORMATION

I understand that my unauthorized use or disclosure of confidential data/information is grounds for immediate disciplinary action. Examples of disciplinary action include termination of all facility and network access, termination of the partnership, and demand for return of all confidential information.

I also understand that my unauthorized use or disclosure of confidential information may be subject to administrative, civil, and criminal penalties identified in law.

_____ _____

Signature of Data User | Print Name of Data User | 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. The **[NAME OF TRIBAL JURISDICTION]** agrees to store data/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 **[NAME OF STATE AGENCY]** and the Information Recipient, access is controlled by the **[NAME OF STATE AGENCY]**, who will issue authentication credentials.

2. Information Recipient will notify **[NAME OF STATE AGENCY]** immediately whenever:

    a) An authorized person in possession of such credentials is terminated or otherwise leaves the employ of the Information Recipient;

b) Whenever a person's duties change such that the person no longer requires access to perform work for this Contract.

3. The data must not be transferred or accessed over the Internet by the Information Recipient in any other manner unless specifically authorized within the terms of the Agreement.

    a) If so, authorized the data must be encrypted during transmissions using a key length of at least 128 bits. Industry standard mechanisms and algorithms, such as those validated by the National Institute of Standards and Technology (NIST) are required.

    b) Authentication must occur using a unique user ID and Complex Password (of at least 10 characters). When the data is classified as Confidential or Restricted, authentication requires secure encryption protocols and multi-factor authentication mechanisms, such as hardware or software tokens, smart cards, digital certificates or biometrics.

    c) Accounts must lock after 5 unsuccessful access attempts, and remain locked for at least 15 minutes, or require administrator reset.

F. Data storage on mobile devices or portable storage media

1. Examples of mobile devices are smart phones, tablets, laptops, notebook or netbook computers, and personal media players.

2. Examples of portable storage media are flash memory devices (e.g., USB flash drives), external hard drives, and portable hard disks.

3. Data must not be stored by the Information Recipient on mobile devices or portable storage media unless specifically authorized within the terms of this Agreement. If so authorized:

    a) The devices/media must be encrypted with a key length of at least 128 bits, using industry standard mechanisms validated by the National Institute of Standards and Technologies (NIST).

        - Encryption keys must be stored in a secured environment that is separate from the data and protected in the same manner as the data.

    b) Access to the devices/media is controlled with a user ID and a Complex Password (of at least 6 characters), or a stronger authentication method such as biometrics.

    c) The devices/media must be set to automatically wipe or be rendered unusable after no more than 10 failed access attempts.

d) The devices/media must be locked whenever they are left unattended and set to lock automatically after an inactive period of 3 minutes or less.

e) The data must not be stored in the Cloud. This includes backups.

f) The devices/ media must be physically protected by:

- Storing them in a secured and locked environment when not in use;
- Using check-in/check-out procedures when they are shared; and
- Taking frequent inventories.

4. When passwords and/or encryption keys are stored on mobile devices or portable storage media they must be encrypted and protected as described in this section.

G. Backup Media

The data may be backed up as part of Information Recipient's normal backup process provided that the process includes secure storage and transport, and the data is encrypted as described under *F. Data storage on mobile devices or portable storage media.*

H. Paper documents

Paper records that contain data classified as Confidential or Restricted must be protected by storing the records in a secure area which is only accessible to authorized personnel. When not in use, such records 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 the Information Recipient, all of the data can be identified for return or destruction. It also aids in determining whether the data has or may have been compromised in the event of a security breach.

2. When it is not feasible or practical to segregate the data from other data, then ***all*** commingled data is protected as described in this Exhibit.

J. Data Disposition

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

Data stored on:	**Is destroyed by:**

Hard Disk Drives / Solid State Drives	Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the data cannot be reconstructed, or Physically destroying the disk, or Delete the data and physically and logically secure data storage systems that continue to be used for the storage of Confidential or Restricted information to prevent any future access to stored information. One or more of the preceding methods is performed before transfer or surplus of the systems or media containing the data.
Paper documents with Confidential or Restricted information	On-site shredding, pulping, or incineration, or Recycling through a contracted firm provided the Contract with the recycler is certified for the secure destruction of confidential information.
Optical discs (e.g., CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a course abrasive.
Magnetic tape	Degaussing, incinerating or crosscut shredding.
Removable media (e.g., floppies, USB flash drives, portable hard disks, Zip or similar disks)	Using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data. Physically destroying the disk. Degaussing magnetic media sufficiently to ensure that the data cannot be reconstructed.

K. Notification of Compromise or Potential Compromise

The compromise or potential compromise of the data is reported to **[NAME OF STATE AGENCY]** as required under the Agreement.

APPENDIX C: CERTIFICATION OF DATA DISPOSITION

Date of Disposition _____

☐ All copies of any Datasets related to agreement **[NAME OF STATE AGENCY]** #_____ 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 **[NAME OF STATE AGENCY]** #_____ 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 **[NAME OF STATE AGENCY]** #_____ have been physically destroyed to prevent any future use of the materials and media.

☐ All paper copies of the information related to the agreement **[NAME OF STATE AGENCY]** #_____ have been destroyed on-site by crosscut shredding.

☐ All copies of any Datasets related to agreement **[NAME OF STATE AGENCY]** #_____ that have not been disposed of in a manner described above, have been returned to **[NAME OF STATE AGENCY]**.

☐ Other

The data recipient hereby certifies, by signature below, that the data disposition requirements as provided in the agreement **[INSERT TITLE OF PUBLIC HEALTH DATA SHARING AGREEMENT],** Section 12, Data Disposition, have been fulfilled as indicated above.

_____ _____

Signature of data recipient Date

APPENDIX D: SMALL NUMBERS GUIDELINES

- **[NAME OF STATE AGENCY]** and **[NAME OF TRIBAL JURISDICTION]** will aggregate data so that the need for suppression is minimal. **[NAME OF TRIBAL JURISDICTION]** has the sovereign authority over its data to self-determine whether and how it will suppress data related to small numbers.
- **[NAME OF STATE AGENCY]** and **[NAME OF TRIBAL JURISDICTION]** will suppress rates or proportions derived from those suppressed counts.
- **[NAME OF STATE AGENCY]** and **[NAME OF TRIBAL JURISDICTION]** 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%).
- **[NAME OF STATE AGENCY]** 's Small Number Standards are posted on the **[NAME OF STATE AGENCY]** website: **[INSERT WEB ADDRESS]**.

APPENDIX E: TRIBAL NATION DATA USE FORM

Timelines for submitting Tribal Nation Data Use Form. The Tribe will respond no later than 60 days after receipt of this form. If the Tribe does not respond within 60 days of receiving **[NAME OF STATE AGENCY]**'s request, the **[NAME OF STATE AGENCY]** request will be deemed approved. **[NAME OF STATE AGENCY]** can request approval prior to 60 days by providing justification for an expedited process. The Tribe form can return this form to **[INSERT STATE AGENCY EMAIL]**.

PART I – To be completed by [NAME OF STATE AGENCY] requesting/notifying entity.

	TO BE COMPLETED BY [NAME OF STATE AGENCY]
1. Date of Request	
2. Name of Contact Person, Title, Program, and Department	
3. Email and Phone	
4. Is this a request for the Tribe's Approval to use the Tribe's data or is this from the Tribe or a Notification to the Tribe? [If this a notification only, please specify the type of exempted use this notification qualifies for under Section 5(e) of the Tribal Data Sharing Agreement]?	
5. Brief title for data use approval request or notification of exempted data use.	
6. Date approval is needed (N/A, if this is a notification of exempted data use).	
7. 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).	
8. One-time use or a recurring use?	
9. Anticipated frequency of use (e.g., daily, monthly, annually, etc.)	
10. Tribal data to which this request or notification applies	
11. How the data will be used (published, analyzed, shared, or used in research or other applications, etc.) and why it is necessary	

12. Who will gain access to these data or to products that include or are derived from this request or notification?	
13. How will data collection occur (e.g., a field in WDRS)	
14. Potential benefits to the Tribal Nation, AI/AN and/or other Tribes	
15. Potential risks or harm to the Tribal Nation, AI/AN and/or other Tribes	
16. Any additional information that will be useful to the Tribal Nation in reviewing this request or notification	

PART II – To be completed by the Tribal Jurisdiction.

	TO BE COMPLETED BY TRIBAL JURISDICTION
1. Date of Response	
2. Name of Contact Person, Title, Program, and Department	
3. Email and Phone	
4. If this is a request for approval by the Tribe, does this Tribe approve or disapprove of the request above?	☐ **Approve** ☐ **Disapprove** ☐ **N/A – This is a notification only**
5. Potential benefits of this request (e.g., consistent with Tribal sovereignty, respects Tribal culture, will help improve health of AI/AN, will help dispel negative racial stereotypes, supports strengthening Tribal public health capabilities)	
6. Potential risks or negatives associated with this request (e.g., inconsistent with Tribal sovereignty, not respectful of Tribal culture, perpetuates negative racial stereotypes, does not support improving health status of AI/AN, may not be sufficient information to prevent incorrect conclusions, does not support strengthening Tribal public health capabilities)	
7. Please explain whether the benefits of this request or notification will outweigh the potential risks or harm.	