

Northwest Tribal Epidemiology Center

Data Governance Handbook

Version 1.1



NORTHWEST PORTLAND AREA
INDIAN HEALTH BOARD
Indian Leadership for Indian Health

Document History

Document Version	Completion Date	Action Type	Brief Description	Authors/Reviewers
0.1	12/11/2023	Document Creation	Completed first draft	S Joshi
0.1	1/19/2024	Review	Internal review by staff	IDEA-NW and Epi & Surveillance Unit staff, Indi Matthew
0.5	2/21/2024	Document update	Addressed comments from internal reviewers	S Joshi
0.5	3/5/2024	Review	NWTEC Director review and comments	Victoria Warren-Mears
1.0	3/21/2024	Document update	Addressed comments from NWTEC Director	S Joshi
1.1	11/1/2024	Document update and review	Updated roles and responsibilities to make more general to NWTEC project directors and staff; updated links to guidance for external data transfers; updated information on tribal data sharing agreements	S Joshi, V Warren-Mears, A Yang, S Stone

Table of Contents

Document History	1
Purpose	4
Scope.....	4
Guiding Values.....	4
Applicable Laws, Policies, and NPAIHB Resolutions	6
Roles and Responsibilities	7
Points of Contact.....	7
Data Management.....	9
Data Asset Inventory	9
Data Protection and Confidentiality	9
Protection of Tribal Data	9
Authorization to Access Data.....	9
Training and Documentation Requirements.....	10
Data Storage and Access.....	13
Data Transfers	16
Data Destruction	16
Protocol for reporting a data breach or loss	17
Data Standards.....	18
Folder and file organization	18
Data Folders on NPAIHB’s servers	18
Analytic Code and Outputs	19
Data Sharing Agreements, IRB Documentation, Training Documents, and Other Administrative Files	19
Data Preparation	19
Linked Datasets.....	19
Metadata and supporting documentation	22
Data Release and Reporting.....	23
Release of Tribe- or Tribal Area-Specific Data	23
Data Sharing Agreements with Tribes	24
Data Request and Technical Assistance processes.....	24
Small Numbers and Data Suppression Guidance	24

Review Requirements for Peer-Reviewed Publications and Conference Presentations and other Data Releases.....	28
Authorship and Co-Authorship Guidelines.....	30
Release of data to the media and through social media channels.....	30
Review and updates to this document.....	32
Future directions for data governance at NPAIHB	33
Appendix A: Security Requirements	35
Appendix B: Instructions for accessing the CITI Human Subjects Training Course.....	37
Appendix C: How to securely shred files.....	38
Appendix E: Templates and other Resources	41
Template Certificate of Data Destruction.....	42
Appendix F: Definitions.....	43
Appendix G: Resolutions and other supporting documentation	45
Resolution 05-04-04: Tribal Ownership of Data	46
Resolution 21-04-03: Linkages with the Northwest Tribal Registry	49
Resolution 21-04-04: NDW Access for Record Linkages.....	52
NWTEC Strategic Framework for Data Modernization.....	54

Purpose

The purpose of this handbook is to support Northwest Tribal Epidemiology Center (NWTEC) staff in managing and stewarding data through the data lifecycle in accordance with the Northwest Portland Area Indian Health Board's (NPAIHB's) mission, values, and policies. It outlines policies and standards to promote the availability, quality, and security of NWTEC's data resources. These policies and standards support data governance. At NPAIHB, the goal of data governance is to maintain and share high-quality data in ways that are secure and accessible to serve the public health data needs of Northwest Tribes.

Scope

The guidance in this handbook generally applies to primary (data collected firsthand by NWTEC programs) and secondary data (data collected by other entities and obtained by NWTEC) utilized for public health surveillance, assessment, and evaluation purposes. Data utilized for research purposes should follow the data management and security protocols outlined in Institutional Review Board (IRB) approved research protocols. If data obtained by NWTEC for public health practice purposes are to be used for research, investigators must submit research applications to the appropriate tribal, regional, and state IRBs and be aware that they may still need to adhere to the data release and reporting requirements outlined in this handbook.

Guiding Values

NWTEC's data governance strategy is informed by NPAIHB's guiding values and the values outlined in NWTEC's Strategic Framework for Data Modernization.

NPAIHB's guiding values¹ are:

- Tribal Sovereignty - The government-to-government relationship and treaty and trust obligations require meaningful tribal consultation on all initiatives impacting tribes and American Indian/Alaska Native (AI/AN) people. Meaningful tribal consultation involves an open exchange of information, discussion and decision-making by tribes and the federal government.
- Traditional Indigenous Knowledge - In Indigenous communities, health and wellness involves multiple facets of life including the environment, space, and health of the earth. Conceptual framework for treating health among AI/AN people should include the dimensions of caring, traditions, respect, connection, holism, trust, and spirituality. Overall, holistic health promotion and disease prevention is the key to the health and well-being of the AI/AN seventh generation and must be included in all initiatives.
- Culture as Health Promotion - Cultural and traditional interventions must be incorporated alongside existing health care promotion efforts to ensure a culturally tailored and culturally relevant approach to health promotion, prevention, and health care delivery for AI/AN people. Inclusion of all community members from our children to our elders will promote wellness and healing across all generations.

¹ From NPAIHB's 2020-2025 Strategic Plan

The values outlined in [NWTEC's Strategic Framework for Data Modernization](#) are:

- Data Sovereignty – We believe in the rights of tribes to define data and populations of focus, and govern the collection, ownership, and application of their own data.
- Capacity Building – We believe in building the knowledge, techniques, and skills of individuals and cultivating effective and enabling institutions (i.e., NPAIHB, Board staff, Board delegates, member tribes' institutions and staff).
- Sustainability – We believe in efficient and impactful use of resources for successful, long-term data modernization.

Applicable Laws, Policies, and NPAIHB Resolutions

The following NPAIHB resolutions inform NWTEC’s data governance strategy:

- [Resolution 05-04-04: Tribal Ownership of Health-Related Data](#) – While this resolution is focused on data collected for research purposes, some of the underlying principles (tribal ownership of data, protection of tribal data against unauthorized use, utilizing IRB review to ensure protection of individuals and communities) apply to NWTEC’s public health surveillance, assessment, and reporting activities.
- [Resolution 21-04-03: Support for NPAIHB EpiCenter Access and Record Linkages with Public Health Surveillance Systems in Idaho, Oregon, and Washington](#) – This resolution supports NWTEC’s work to access and link with public health surveillance systems in Idaho, Oregon, and Washington.
- [Resolution 21-04-04: Support for NPAIHB EpiCenter Access to the Indian Health Service’s National Data Warehouse Data for Record Linkages](#) – This resolution supports NWTEC’s access to IHS National Data Warehouse data to create the Northwest Tribal Registry (NTR) file for use in correcting AI/AN racial misclassification in data systems.

In addition, NWTEC staff must adhere to all policies and provisions in NPAIHB’s Program Operations Manual (POM), including provisions for:

- retention of program files (section 2.2).
- ensuring data security and confidentiality for teleworking employees (section 4.3.J).
- release of confidential information (section 10.3).
- intellectual property and product ownership (section 10.4).
- scientific misconduct (section 14).
- financial conflict of interest (section 15).

NWTEC staff must also comply with state and federal laws that govern the confidentiality and security of information for specific data systems. These requirements are summarized in [Appendix A: Security Requirements](#) and are also specified in data sharing agreements (DSAs)² and confidentiality agreements for specific systems. These agreements can be accessed at: [P:\IDEA-NWIRB and DSAs](#).

² In this document, the term “data sharing agreement” is used broadly and includes other types of agreements that govern the exchange of data between NWTEC and tribal, state, and federal entities. These types of agreements include data sharing agreements, data use agreements, memoranda of agreement, memoranda of understanding, etc.

Roles and Responsibilities

The key roles for implementing NPAIHB’s data governance strategy, and their general responsibilities, are outlined in the table below.

Role	Responsibility with regards to Data Governance
NWTEC Data Analysts and Evaluators	<ul style="list-style-type: none"> • Ensure NWTEC data is managed and stewarded in accordance with the policies and standards outlined in this handbook and in other documents that govern data use and release (e.g., tribal, state, and federal DSAs). • Complete required confidentiality training and agreements when requested by their supervisor. • Promptly report any incidents that result in a data loss, data breach, or inappropriate release of data to their supervisor or the NWTEC Director. • Participate in activities to promote and strengthen data governance at NWTEC.
NWTEC Project Directors	<p>Responsibilities include those listed under Data Analyst and Evaluators and:</p> <ul style="list-style-type: none"> • Coordinate training, communications, and other activities to support the implementation of policies and standards outlined in this handbook. • Review analytic datasets, methods, code, and products to ensure quality, security, and adherence to policies and standards. • Regularly review and update this handbook. • Support the NWTEC Director in responding to any incidents that result in a data loss, data breach, or inappropriate release of data.
NWTEC Director	<ul style="list-style-type: none"> • Provide oversight for the development and implementation of NWTEC’s data governance strategy. • Lead responses to incidents that result in a data loss, data breach, or inappropriate release of data.
NPAIHB Information Technology (IT) Department	<ul style="list-style-type: none"> • Support NWTEC staff in ensuring that NPAIHB’s IT infrastructure meets requirements for accessing, transmitting, storing, and destroying data. • Provide input to NWTEC staff on strategies to promote and optimize data security at NWTEC.

Points of Contact

The current points of contact for the positions and roles described in this document are:

- NWTEC Director: Victoria Warren-Mears, PhD
- Epidemiology & Surveillance Unit Project Director: Alyssa Yang
- IDEA-NW Project Director: Sujata Joshi

- Data Hub Outreach Manager: Sunny Stone
- NPAIHB IT Department
 - IT Director: Marches Armstrong
 - Network Administrator: Jamie Alongi
 - Network Support Tech: Jason Arnold

A description of the roles and responsibilities for IT staff members can be found on the [IT Department SharePoint site](#).

Data Management

Data Asset Inventory

An inventory of data assets managed by the IDEA-NW project and Epidemiology & Surveillance Unit is saved in this location: <\\192.168.2.34\Epicenter\IDEA-NW\IDEA-NW Dataset Tracker.xlsx>

The inventory includes information on datasets available by state/agency, years available, status of analytic datasets, and expiration dates of DSAs with state and federal data systems. The inventory is updated as new data are obtained and as DSAs are completed or renewed.

Data Protection and Confidentiality

Protection of Tribal Data

As stated in Section 10.3 of NPAIHB's POM:

The release of confidential records maintained by NPAIHB in violation of the Privacy Act of 1974 (Title 5 US Code), Privacy Act Regulations (45 CFR, Part 5b), and NPAIHB policy is prohibited and subject to disciplinary action.

It is the policy of the NPAIHB that requests from NPAIHB employees for tribal data necessary to complete NPAIHB Projects are to be made in writing to the tribal council. The request must include a statement of how the data is to be used, a list of users, a description of how confidentiality will be maintained, and a sample resolution and/or data sharing agreement authorizing the release of the data. The Executive Director must approve all requests. Records obtained for NPAIHB projects that contain personal or tribal specific information are to be protected from uses other than those for which they were collected and be accessible only to those assigned to the project. Personal and tribal specific information is not to be disclosed without prior written consent of the individual or tribal government. Confidentiality must be maintained by NPAIHB employees so that the relationship and reputation of NPAIHB with its member tribes and with other agencies is not jeopardized, and the reliability of data is not questioned.

For additional guidance on the release of tribal data, see the [Release of Tribe- or Tribal Area-Specific Data](#) and [Data Sharing Agreements with Tribes](#) sections.

Authorization to Access Data

Access to datasets that contain record-level personally identifiable information (PII) and protected health information (PHI) is restricted to the minimum number of individuals who require access to data to complete their job functions. The NWTEC director and NWTEC project directors are responsible for determining the appropriate levels of access for NPAIHB staff, contractors, consultants, and interns.

NPAIHB Staff

In general, NWTEC staff in the roles of analysts (i.e., epidemiologists, biostatisticians, informaticians, evaluators) require access to record-level PHI to complete their job functions. The

supervisory project director should ensure these staff complete required confidentiality trainings and documentation, are granted access to the appropriate server folders, and comply with internal and external policies related to data release, reporting, and publication. A very limited number of staff persons require access to PII data contained in the Northwest Tribal Registry (NTR); the IDEA-NW project director determines which staff require access to these data. Access to data contained in the Northwest Tribal Data Hub is authorized by the IDEA-NW project director using the appropriate standard operating procedures³. All documentation related to the Data Hub are stored at <https://npaihb1.sharepoint.com/sites/NPAIHBDataHub> and can be requested from the IDEA-NW Project Director or Data Hub Outreach Manager.

Contractors, Consultants, and Interns

Contractors, consultants, and interns are expected to adhere to internal and external policies for protecting data and maintaining confidentiality. At a minimum, the supervisory project director must be informed if access to record-level PHI data is needed for these individuals. Individuals with short-term or limited scope engagements with NWTEC may be considered exempt from some training and documentation requirements. NWTEC staff who provide oversight for these individuals must ensure contractors, consultants, and interns complete appropriate training and documentation requirements and provide oversight for individuals' actions with regards to data.

Audits

At least annually, the IDEA-NW project director will work the NPAIHB's IT department to conduct an audit of the following:

- Staff members need to access restricted access folders containing PHI data from tribes and state and federal agencies.
- Current listing of staff members with access to restricted access folders containing PHI data.
- Staff members' completion of required confidentiality training and documentation.

Audits for the Northwest Tribal Data Hub will be conducted in accordance with [Data Hub standard operating procedures](#).

Training and Documentation Requirements

Individuals with access to NWTEC-managed PHI and PII data must complete data security and confidentiality training and documentation. This is to ensure that individuals with access to NWTEC-managed assets: 1) receive training to understand and apply requirements for protecting confidential data, and 2) meet the training and documentation requirements of external entities (i.e., the Portland Area IRB; tribal, state, and federal agencies). These requirements apply to NWTEC staff, interns, contractors, and other individuals with access to NWTEC-managed data assets.

- At the time of hire, all NPAIHB staff must read and complete training on the Scientific Misconduct and Financial Conflict of Interest policies included in NPAIHB's POM.

³ As of October 2024, the standard operating procedures and documentation for the Northwest Tribal Data Hub are under development.

- All NPAIHB staff, contractors, and interns must complete training required by NPAIHB’s IT department when requested.
- Additional training and documentation requirements for specific data asset classes are outlined in the table below.

Table 1. Training and documentation requirements by asset class.

Data Asset Class	Applies To	Exceptions	Training Requirement	Frequency	Documentation Requirement
A) Tribal, State, and Federal data utilized for public health assessment, surveillance, or research	Staff, interns, contractors, external collaborators who access data for the purposes of data management and/or analysis	Some contractors and interns with short-term and/or limited scope engagements that do not require access to record-level data may be considered exempt from some requirements. At a minimum, these individuals must complete the NWTEC Data Confidentiality Pledge and any security training required by NPAIHB’s IT department. Consult with the supervisory project director to determine additional training or documentation	A1. Read and sign NWTEC Data Confidentiality Pledge_General	Within one month of date of hire and then annually	Copy of signed confidentiality pledge
			A2. Complete all modules of Indian Health Service Information Security Systems Awareness (ISSA) Training	Within one month of date of hire and then annually	Copy of ISSA Certificate
			A3. Complete Human Subjects Research training from an approved training provider ⁴	Within two months of date of hire and then every three years	Copy of training certificate
			A4. Read data confidentiality and reporting requirements for individual data systems/sets (as outlined in DSAs), and complete additional confidentiality requirements	As needed/ requested	Copies of system-specific confidentiality agreements

⁴Approved training programs include the University of Washington [Research Ethics for Health in Indigenous Communities \(rETHICS\)](#) or [CITI Program](#) (see [Appendix B](#) for information on accessing the CITI training for no cost)

		for these individuals.	for those systems		
B) Indian Health Service (IHS) Epi Data Mart (EDM)	Staff, interns, contractors, external collaborators who access data for the purpose of data management and/or analysis	No exceptions	B1. Complete requirements A1 and A2	Within one month of date of hire and then annually	Copy of agreement/ training certificate
			B2. Complete IHS HIPAA training	When first requesting access	Copy of training certificate
			B3. Read and sign Individual Rules of Behavior (ROB) Regarding Appropriate Use of EDM Limited Datasets ⁵	When first requesting access and then annually	Copy of signed ROB
			B4. Complete TEC Affiliation Status Letter	When first requesting access	Copy of signed Affiliation Verification Letter
C) Northwest Tribal Registry (NTR)	Staff who access data for the purpose of preparing and utilizing the NTR for record linkages	No exceptions	C1. Complete all modules of Indian Health Service Information Security Systems Awareness (ISSA) Training	One month prior to requesting access to the NTR and then annually	Copy of training certificate
			C2. Read and sign the NTR Confidentiality Pledge	One month prior to requesting access to the NTR, and then annually	Copy of signed confidentiality pledge
			C3. Complete IHS HIPAA training	One month prior to requesting access to the NTR	Copy of training certificate

⁵ Request from the IDEA-NW project director if you're unable to access the form.

			C4. Obtain authorization from IHS to access the NTR file	One month prior to requesting access to the NTR	Copy of email/letter authorizing access
D) Northwest Tribal Data Hub	All individuals receiving credentials to the Data Hub	No exceptions	D1. Sign Data Hub Terms and Conditions	Upon initial credentialing and then annually	Copy of signed Data Hub Terms and Conditions

- The supervising project director will communicate training requirements to new hires.
- The IDEA-NW project director will send annual reminders to existing staff seeking to renew their access to the data asset classes above.
- Staff who require access to one or more of the above data asset classes (for themselves or for interns or contractors) are responsible for notifying the IDEA-NW or Epidemiology & Surveillance Unit project director with information about the data asset(s) needed, timeframe within which access is needed, and when access is no longer needed (if before the end of employment/engagement with NPAIHB).
- The IDEA-NW project director will maintain a [tracking sheet](#) that documents the completion of training requirements for each individual, and will make this tracking sheet available to NPAIHB leadership and staff and external partners upon request.
- To the extent possible, new and existing staff will be allowed one month to complete training and documentation requirements (or two months for human subjects training).

Data Storage and Access

NPAIHB servers

NPAIHB’s servers are maintained by NPAIHB’s IT department and have the following features:

- Access to servers is restricted to NPAIHB IT staff and the Operations Director. Servers are in a locked room within NPAIHB’s offices. Only authorized staff (including members of NPAIHB IT department and NPAIHB’s Operations Director) have key fobs to unlock the server room.
- Files on NPAIHB’s servers are backed up:
 - Locally twice a day at 7 am and 12 pm
 - To an external on-site storage device every night at 7 pm
 - Weekly to a secure off-site location
- Servers are not encrypted.

Requirements for Network Access

To access information stored on NPAIHB’s network servers, users must:

- Utilize a NPAIHB-issued computer.
- Access the server either on-site at NPAIHB’s office or through NPAIHB’s virtual private network (VPN) service.

- Access the server using a unique user ID and a password that meets NPAIHB’s password requirements:
 - Passwords must be at least 8 characters in length and meet the following requirements:
 - Cannot contain the user’s login/account name.
 - Must contain characters from three of the following categories:
 - Uppercase letters
 - Lowercase letters
 - Base 10 digits (0-9)
 - Non-alphanumeric characters
 - Passwords must be changed every 90 days for NPAIHB staff and contractors with network access.
- Multi-factor authentication is required to access Office365, when a new device is being used, or a password has been changed.

Storage of PHI and Tribal Data on NPAIHB’s servers

Files containing record-level PHI from any source or files containing tribal data (record-level or aggregated) are stored in a restricted access location on NPAIHB’s servers. Restricted access locations are folders or drives that are only accessible by designated individuals. NPAIHB’s IT department creates restricted access locations and updates user access lists upon request. All record-level PHI data (from tribal, state, and federal agencies) and aggregated tribal data is stored in restricted access server locations, as noted below. Access to these folders must be approved by the NWTEC Director.

The following restricted access folders are currently used to store PHI data obtained from tribes and state and federal agencies:

- P:\IDEA-NW Data
- P:\IDEA-NW
- P:\EDM
- P:\CDC COVID Case Surveillance Data

Note: Please refer to the [File and Folder Organization](#) section of the document for guidance on saving and organizing data and other files.

Storage of PHI and Tribal Data on individual computers

Storing local copies of PHI and tribal data on individual computers is not advised but may be necessary in some cases. Prior to downloading and storing data on individual computers, analysts must ensure:

- Computers are encrypted using a 256-bit Advanced Encryption Standard (AES-256) algorithm that is validated by the National Institute of Standards and Technology (NIST).
 - NPAIHB currently uses BitLocker to encrypt computers. BitLocker meets the above requirements for encryption.

- Users utilize a unique user ID and complex password to login to their computers.
 - NPAIHB staff with encrypted computers must first enter a passcode to decrypt their computers and then use their unique user ID and password that meets NPAIHB's password requirements to login to their computer.
- Users destroy the data files using the [secure shred function](#) on their computer after analysis completion.

Storage and Use of Personally Identifiable Information/NTR files

The NTR contains PII data used to conduct linkages with state datasets. The NTR is stored on a stand-alone linkage laptop that includes BitLocker whole disk encryption that utilizes an AES 256-bit encryption algorithm with FIPS 140-2 Operational and Integrity checks enabled. After decrypting the hard drive using a passcode, users must utilize a password that meets NPAIHB's password requirements to access the local drive. To access the NTR, users must mount an encrypted virtual disk located on the computer's hard drive using a complex password. In addition, the following security measures are utilized:

- When the NTR file is being utilized during linkages, staff will ensure that the laptop is unconnected to any public network, including internet access, until the linkage is completed.
- The laptop will be stored in a fireproof safe at NPAIHB when not in use. The safe is in an office shared by the IDEA-NW and Epidemiology & Surveillance Unit project directors; the office will be locked when not in use.
- A log, located near the safe, will be used to document removal and return of the laptop from the safe.
- While traveling, the laptop shall always remain in the possession of the staff member.
- When confidential files need to be destroyed, they shall always be deleted via secure shred function. This function ensures complete destruction of files without leaving fragments that can be recovered.
- Back-ups of the most recent version of the NTR file will be saved to an encrypted flash drive. The flash drive will be stored in a NPAIHB safe located offsite.
- Access to the linkage laptop will be limited to the minimum staff members necessary to complete linkages. These staff members must be approved by the IDEA-NW project director and complete the required training and authorization needed prior to accessing the laptop.

Additional information on accessing the safe used to store the linkage laptop and the encrypted flash drive with backups of the NTR file can be found in this document: [Storage and Backups for NTR and Linkage Laptop](#)

Storage of data in the Cloud

The security requirements outlined in [Appendix A: Security Requirements](#) apply to data stored in the Cloud. The specific applications of these requirements to the Northwest Tribal Data Hub are outlined in documentation stored at <https://npaihb1.sharepoint.com/sites/NPAIHBDataHub>.

Data Transfers

Appropriate agreements, such as completed DSAs, must be in place before data transfers occur.

State & Federal: Most data provided by state or federal agencies are accessed through secure data portals or secure file transfer sites operated by the agency. These sites should be utilized when retrieving or transferring data with these agencies.

Tribal & Other: For data transfers with tribes or other partners, the preferred method of transferring datasets with confidential information is to utilize NPAIHB's guidance for sharing externally using SharePoint. Follow the steps provided in the guidance document [Sharing Externally with SharePoint](#).

Data Destruction

When should data be destroyed?

- Surveillance & ongoing data: In general, NWTEC may retain data files obtained from tribal, state, and federal agencies if we have an active data sharing agreement in place with the data provider.
 - Please refer to the specific agreements that govern data access and retention for additional guidance on when data should be destroyed.
- Project-specific data: For tribal data shared with NWTEC for specific analytic projects:
 - Please refer to the data sharing agreement for guidance on when data should be destroyed or returned to the Tribe.
 - Verify that your collaborators have received, saved, and successfully opened all required files and outputs from the project. Also verify that they do not need NPAIHB to retain or store any copies of the data on their behalf.
 - If no such guidance is available, follow up with your contact at the Tribe at the project's end to identify their preference for destroying NWTEC's copies of their data.
 - If tribal data were transferred to NWTEC electronically (e.g., through SharePoint or other file sharing service), ensure that the copies stored on those platforms are also permanently destroyed.

Procedures for destroying data

- Data files stored on NPAIHB's servers can be destroyed by deleting the file from its server location. However, be aware that the files are still recoverable for a year (365 days) after deletion due to server backups.
- Data files stored on individual computers can be permanently destroyed using a [secure shred function](#).
- Data files stored in the AWS Cloud environment as part of the Data Hub must be destroyed according to [standard operating procedures for the Data Hub](#).

Documenting Data Destruction

- It is recommended to document instances when all copies of a particular data file are permanently destroyed. The requirements for documenting and reporting data destruction

vary by data provider. Please refer to the data sharing agreement for a particular data system to understand these documentation and reporting requirements.

- Some data providers (e.g., the Washington Department of Health [DOH]) provide a specific form to complete when reporting the destruction of data files (provided as an appendix in Washington DOH data sharing agreements). In cases where a specific form isn't provided, [NPAIHB's Certificate of Data Destruction](#) can be used to report the destruction of data files.

Protocol for reporting a data breach or loss

In the event of any known or suspected loss of sensitive information (including record-level PHI or PII data, record-level tribal data, or aggregated tribal data), project staff will take the following steps:

1. Staff will notify NWTEC Director, who will notify NPAIHB's Executive Director.
2. If the loss involves a stolen computer or a hacking incident, the appropriate public safety personnel for the jurisdiction will be notified by the staff person in possession of the computer at the time of its theft. Project staff will provide public safety personnel with the computer's serial number during the initial theft report or during a follow-up call. Project staff will request a theft report, which will be held on file by the supervisory Project Director.
 - a. Computer serial numbers are held on file by NPAIHB's IT department and are available within 24 hours.
3. The NWTEC Director will notify owners of the data, the points of contact on signed data sharing agreements, and/or co-investigators of the loss/theft within one (1) week of the loss with a written communication, unless otherwise stated in signed data sharing agreements or otherwise directed by public safety personnel or IRB.
4. If the loss involves data used for or obtained through linkages, or research data collected under an IRB protocol, the NWTEC Director or their designee will notify the Portland Area Office of the Indian Health Service IRB through the IRBNet (by filing a serious adverse event notification), or via face-to-face contact with the IRB support staff.
5. If the stolen computer or drive is recovered, further notification of the data owners will occur by the NWTEC Director.
6. The NWTEC Director, in consultation with the Executive Director of NPAIHB, will be the point of contact for all communications.

Data Standards

This section describes recommended standards to ensure quality, consistency, and ease of use for NWTEC data assets.

Folder and file organization

Data Folders on NPAIHB's servers

Datafiles should be saved in restricted access folders per the guidance outlined in [Storage of PHI and Tribal Data on NPAIHB's servers](#). Data folders should be organized so that the data and supporting documentation are easy to identify, navigate, and (when necessary) destroy. The guidance below describes recommendations for organizing data folders.

- In general, parent folder names should be descriptive and include the data provider's jurisdiction and type of data. For example:
 - Oregon PRAMS data should be saved under the OR PRAMS data folder.
 - Washington communicable disease data should be saved under WA Communicable Diseases.
 - Tribal community health assessment (CHA) data should be saved in a folder named <Tribe Name> CHA.
- Some datasets are saved under parent folders named with the data type, with subfolders organized by providing jurisdiction. Cancer, death certificate, birth certificate, and hospital discharge data are organized in this way.
- The next level child folder should be organized by one of the following (in order of preference): (1) year(s) of data included in the data file or (2) linkage or acquisition date.
- The next level child folder(s) should be organized as follows:
 - For data obtained through linkages, data should be organized in the following sub-folders:
 - Original Data
 - This folder should include the original files obtained from the data provider prior to any transformations. Include any accompanying metadata and supporting documentation (e.g., data dictionaries, data descriptions) in this folder.
 - Linkage
 - This folder should include any output files retained from the linkage, including the export of linkage flags, accompanying SAS code, and process notes. The summary linkage reports produced from each linkage should also be saved in this folder.
 - SAS Code
 - This folder should only include the SAS (or other programming language) scripts that are used to prepare or modify the analytic files.
 - Analytic Dataset
 - This folder should include the final analytic file prepared for analysis and any accompanying supporting metadata and support documents.

- Note that for datasets where new years of data are appended to existing datasets, the Analytic Dataset folder may be stored in a higher-level folder.
- When relevant, a sub-folder named Archive can be created to store older copies of analytic datasets.
- For data not obtained through linkages or that don't undergo transformations, the folders should include the original dataset and any accompanying metadata or documentation provided.

Analytic Code and Outputs

To avoid clutter and support ease of access, analysis code sets and analytic outputs (e.g., frequency outputs, workbooks, draft, and final data products) should not be saved in the folders containing analytic datasets. In most cases, these files should still be saved in restricted access folders on the server to ensure that aggregated data requiring suppression are not widely accessible. We recommend saving code and outputs in the following locations, based on the type of project:

- Data requests and technical assistance (DRTA)
 - Files should be saved according to the guidelines documented in the [Protocol for DRTA Process](#) guidance document.
- Presentations
 - Files can be saved in a sub-folder with a descriptive name in the [Presentations abstracts folder](#).
- Publications and Reports
 - File can be saved in a sub-folder with a descriptive name in the [Publications folder](#).

Data Sharing Agreements, IRB Documentation, Training Documents, and Other Administrative Files

For data managed by the IDEA-NW and Epidemiology and Surveillance Unit, administrative documents such as state and federal DSAs, IRB approvals, and documentation of staff confidentiality training are saved under the [IDEA-NW IRB and DSAs](#) folder. Documents are organized under descriptive folder names that indicate the type of documents stored in the sub-folders.

DSAs with tribes are saved in the [Data Sharing Agreements](#) folder on NPAIHB's SharePoint.

Data Preparation

Linked Datasets

Datasets that have been linked with the NTR should undergo data preparation steps to include the core variables listed in the table below. These variables are the minimum needed to evaluate misclassification and calculate descriptive statistics and age-adjusted rates by race, sex, and geographic unit. Note that some datasets may deviate from the values listed in the table due to issues with the data available in original or historical files. We recommend following the coding logic in the preparation code set to ensure consistency across years.

To the extent possible, retain as many of the variables available in the original data file. If newer years of data include variables not provided in previous years' data, retain these variables, and indicate the years they are available in the data dictionary for the post-linkage dataset.

Table 2. Core variables for linked datasets.

Variable Name	Values	Format
Age	Continuous variable, range depends on dataset. Code whole integers only (i.e., 0,1,2,3,etc). Code missing values as 999.	Numeric
Agegroup	5-year age groups, 18 categories, starting with '00-04' and ending with '85+'. The coding should look like: If $0 \leq \text{age} < 5$ then agegroup = '00-04'; else If $5 \leq \text{age} < 10$ then agegroup = '05-09'; else... Etc. In other words, the highest age in the 00-04 age group should be 4.999999.	Character
AI/AN	Dichotomous variable indicating for post-linkage AI/AN vs. Non-AI/AN 0 = Non-AI/AN 1 = AI/AN	Numeric
DOB (and other date variables)	Check previous years' analytic file/data dictionary and code accordingly. The default is a numeric value with format MM/DD/YYYY. If some date parts are not available, code as character with the missing part as 99 (e.g., 11/99/2015) If the full date is not available, code as MMYYYY or YYYY (character)	Numeric or character
FIPS_State	Two digit national FIPS code. Oregon = 41 Idaho = 16 Washington = 53 Notes: Some datasets provide a state FIPS code, but these are not the standard FIPS codes specified above. You will need to recode or drop the original variable.	Numeric

	<p>If the state provides information on state/county of residence AND state/county of occurrence, include both variables with a descriptive name (e.g. FIPS_State_res, FIPS_State_occ) and note this in the Read Me document.</p>	
GeoID	<p>Concatenation of state and county FIPS codes; set missing values to state_FIPS 999 (e.g., 41999 for Oregon)</p> <p>Example: Clatsop County (county_FIPS = 007) in Oregon (state_FIPS = 41) has geoid =41007.</p> <p>If the state provides information on state/county of residence AND state/county of occurrence, include both variables with a descriptive name (e.g. GeoID_res, GeoID_occ) and note this in the Read Me document.</p>	Numeric
Hispanic	<p>Ethnicity: 1 = Hispanic (any Hispanic – combine Hispanic codes if needed) 0= Non-Hispanic 9 = Missing/Unknown</p>	Numeric
ID	<p>Unique ID Variable</p> <p>If possible, retain the original value provided by state, but make sure that the ID is unique for the state, year, and record. For birth and death certificates, states repeat the record numbers each year. You may need to concatenate multiple variables (e.g., state, year, certificate number) to create a unique ID. Check existing analytic file or data dictionary.</p>	Character
Match_Status	<p>NTR Match Status: 1 = Match . (missing) = Non-match</p>	Numeric
Misclass	<p>AI/AN Misclassification Status: 1 = Misclassified as non-AI/AN All other values = missing</p>	Numeric
Orig_Hispanic	<p>Original Hispanic variable - retain values provided by state and include coding values in the data dictionary. Check existing analytic file or data dictionary.</p>	

Orig_Race	Original race variables – retain values provided by state and include coding values in the data dictionary. If there are multiple race variables with useable information, recode these as Orig_Race1, Orig_Race2, etc. Check existing analytic file or data dictionary.	
PrelinkRace	Race prior to NTR linkage: 1 = AIAN (any mention of AI/AN or tribal membership in any race/tribal designation field) 2 = NHW (no mention of Hispanic ethnicity in orig_Hispanic field, white with no other race indicated in the original race fields) 9 = Other/Missing/Unknown	Numeric
Race_recode	Race after NTR linkage: 1 = AIAN (any mention of AI/AN or tribal membership in any race/tribal designation field, plus records where match_status = 1) 2 = White (white with no other race indicated in the original race fields) 7 = Other 9 = Missing/Unknown	Numeric
Race_recodeNHW	Race after NTR linkage , AI/AN and NHW only 1 = AIAN (see definition above) 2 = NHW (see definition above, limit to Hispanic = 0) 9 = Other/Missing/Unknown	Numeric
Sex	'M' = Male 'F' = Female 'T' = Trans(gender) (If available) ' ' = Other/Missing/Unknown	Character
Sex_num	1 = Male 2 = Female 3 = Trans(gender) (If available) 9 = Other/Missing/Unknown	Numeric
State	State abbreviations: Oregon = 'OR' Idaho = 'ID' Washington = 'WA'	Character
Year	Year of event (birth, death, diagnosis)	Numeric

Metadata and supporting documentation

Datasets that have been linked with the NTR and undergo data preparation should include a detailed data dictionary and (when appropriate) a READ ME document outlining details that are important for analysts to know (e.g., differences in data availability and variables across years,

major transformations [e.g., when records have been deleted from the original data], etc.). Datasets that have not been transformed should include any documentation provided by the data provider.

Data Release and Reporting

Release of Tribe- or Tribal Area-Specific Data

- Data on individual tribes or individual tribal service areas may only be released with permission from the authorizing official (or alternate) specified in the Tribe’s DSA with NWTEC⁶. Under no circumstances should tribe-specific data be released to entities outside of that Tribe without the Tribe’s written permission.
 - Some tribes’ clinics and programs are operated by the IHS, and staff from these clinics may request tribe-specific data to support their programs. Be aware of these instances and ensure that you do not inadvertently release tribal data to IHS employees serving in these clinics without the tribe’s permission. Be especially careful when there are multiple people included in email messages. Only release data to individuals employed by the Tribe and who are authorized to receive the data.
 - Similarly, be careful of releasing data to contractors or consultants working with tribal programs.
 - For Data Request Technical Assistance (DRTA) responses outside of the Data Hub - It is preferable to have a DSA between the Tribe and NPAIHB in place before releasing data to the Tribe. However, being responsive to Tribes’ requests takes priority – therefore, it is permissible to provide Tribes with data without a DSA in place. In these cases, analysts should connect the requesting Tribe to the Data Hub Outreach Manager, IDEA-NW Project Director, or Epidemiology and Surveillance Unit Project Director to begin the process of establishing a DSA with the Tribe. See the [Data Sharing Agreements](#) section of this handbook for more guidance on this topic.
- Data on sub-state geographic regions that encompass multiple Tribes may also require written permission from those Tribes or a DSA prior to data release. Consult with your supervisor or the NWTEC Director to determine the appropriate approach for releasing data on multiple tribes.
- When entities outside of a Tribe request Tribe-specific data, NPAIHB staff can provide one or more of the following options to respond to their request (depending on staff capacity to respond to the request):

⁶As of the October 2024 update to this handbook, NWTEC has started outreach to tribes to establish updated DSAs using newly approved templates, which include this requirement. As tribal DSAs are being established, analysts responding to tribal DRTA requests should continue responding to and providing data to tribal staff, as long as those responses follow the guidance in this and other sections of the handbook.

- The Tribe can request the data directly from NPAIHB and then release the data to the entity.
- The entity can inform the Tribe of their need for data and request the Tribe provide written authorization for NPAIHB to release Tribe-specific data to the entity.
- The entity, Tribe, and NPAIHB can establish a multi-party DSA that governs the release of data.

Data Sharing Agreements with Tribes

In October 2024, NWTEC's templates and processes for establishing DSAs with individual Tribes were updated. The DSA templates and SOPs for outreach, establishment, and storage of DSAs are saved at [the DSA Templates and Information](#) on NPAIHB's SharePoint.

NWTEC aims to have a current DSA in place with each of NPAIHB's member tribes. The following guidance should be followed:

- A DSA and Data Hub addendum (Addendum A) are required for tribes to access the Northwest Tribal Data Hub.
- A DSA and General Data Exchange addendum (Addendum B) are required for any exchange of tribally-collected data between a Tribe and NWTEC.
- A DSA is preferred but currently not required for DRTA responses. In cases where a tribal DSA is not in place, analysts should connect the requesting Tribe to the Data Hub Outreach Manager, IDEA-NW Project Director, or Epidemiology and Surveillance Unit Project Director to begin the process of establishing a DSA with the Tribe.

There is no current requirement to have a DSA in place to share aggregated state and federal data back with tribes, as long as the data are released in accordance with the guidance outlined in [Release of Tribe- or Tribal Area-Specific Data](#).

The IDEA-NW and Epidemiology & Surveillance Unit Project Directors and the NWTEC Director can help with scoping and developing DSAs.

Data Request and Technical Assistance processes

Responses to DRTA requests should follow the processes and conventions outlined in the [Protocol for DRTA Process](#) guidance document. When possible, internal and external data requestors should be directed to the online form located on [NPAIHB's Data Request and Technical Assistance](#) webpage.

Small Numbers and Data Suppression Guidance

- The NWTEC's data suppression guideline for reporting aggregated data is to suppress all non-zero counts below five, as well as any rates or proportions calculated using a count less than five.

- NWTEC analysts are expected to use caution and judgement when analyzing and reporting data with cell sizes less than 10, particularly at geographic resolutions below the state level and/or for rare conditions.
- When presenting data, ensure that suppressed cells cannot be recalculated through subtraction of non-suppressed cells from totals. Use aggregation (i.e., combine additional years, demographic categories, or geographic areas) to increase cell sizes above suppression thresholds or use secondary suppression (i.e., suppress one or more additional cells) to ensure suppressed cells cannot be re-calculated.
- Some state and federal systems require a higher suppression threshold. The table below outlines suppression guidelines and other restrictions on data release for these systems.

Data Source/System	Suppress non-zero counts below...	Additional guidance on data suppression
CDC Covid-19 Case Surveillance and Vaccination Data	10*	*If the total number of cases in a jurisdiction (i.e., county or group of counties) for a given year and disease/condition is small (i.e., fewer than 10), then race and ethnicity or other indirect identifiers will be suppressed appropriately for all cases in that jurisdiction for that year.
CMS Data provided through the Tribal Data Learning Community	11	
Idaho ESSENCE	5	<ul style="list-style-type: none"> • Ensure that individuals cannot be identified. • Ensure that individual hospitals cannot be identified unless you've received permission from hospital first. When presenting aggregate data, must present information where the number of hospitals must be two or more. • Do not download line-level data, even for internal use.
Oregon ESSENCE	5	<p>The following cannot be disseminated or reported:</p> <ul style="list-style-type: none"> • Names • All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo codes. However, the initial three digits of a zip code may remain on the information if, according to

		<p>current publicly available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic unit containing 20,000 or fewer people is changed to 000.</p> <ul style="list-style-type: none"> • All elements of dates (except year) for dates directly relating to an individual, including birth date, dates of admission and discharge from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of ‘age 90 or older’ • Medical record numbers or any other unique identifying number, characteristic, or code • Data from a sole health care facility or health care system (reports must aggregate data from two or more health systems)
<p>Oregon PRAMS</p>	<p>In general, suppress when:</p> <ul style="list-style-type: none"> • The denominator of a health statistic is 50 or less when the denominator is a population (a group of people with certain age, race, and sex characteristics who live in a particular place) • The denominator is a cohort and the numerator is 10 or 	<p>The Ten and Fifty guideline does not need to be followed in the following cases:</p> <ul style="list-style-type: none"> • When releasing the total number of births or deaths at the county and sub-county level for any time period • When releasing birth or death data for demographic data items at the county or sub-county level for any time period • When releasing birth or death data for non-demographic data items at the county or sub-county level aggregated over three or more years • Rates and percentages from complete count data and registry

	less (a cohort is a group of people whose membership is defined by the occurrence of some event)	data may be published without program review when there are five (5) or more events in the numerator. Unless precluded by confidentiality policies or other program-specific concerns, the small numbers themselves may be published, especially when they represent a sentinel event
Oregon Violent Death Reporting System	10	
WA BRFSS	<ul style="list-style-type: none"> • Suppress data if cell sizes less than 50 or relative standard errors greater than 25% because of unreliability 	
Washington Community Health Assessment Tool	<ul style="list-style-type: none"> • Suppress non-zero counts which are less than 10, and rates or proportions derived from suppressed counts, unless they are in a category labeled “unknown”. 	See Washington DOH’s Reporting Small Numbers guidance
Washington Healthy Youth Survey	<ul style="list-style-type: none"> • Suppress simple frequencies when there are fewer than 15 valid surveys AND • Suppress cross tabs when there are less than five valid responses per cell at the state level or less than 10 valid responses per cell at the sub-state level 	NPAIHB shall obtain written permission from the principals of each school for which NPAIHB will report data in such a way that the school can be identified and written permission from the superintendent of each school district for which NPAIHB will report data in such a way that the school district can be identified. School principal/superintendent permission will not be necessary to use the data to compose groups of schools (e.g., north and south areas of the county) as long as data are not reported in such a way that schools or school districts can be identified. Generally, if there are at least 3 schools and 3 school districts at a geographical level for which data are

		being reported, the schools and school districts are not identifiable. However, there may be exceptions in which they would be identifiable. For example, if the report includes thresholds that all of the schools in a grouping meet (for example, if all schools or school districts in a grouping have especially high or low levels of risk on a particular measure) then the information for those schools or school districts is identifiable, and school principal or superintendent permissions will be obtained.
Washington PRAMS	10	<ul style="list-style-type: none"> Do not publish results at the county level if the total number of respondents in the dataset for the county is less than 50. Do not publish results if the number of participants in each analysis is less than 30.
Washington ESSENCE/RHINO	10	<ul style="list-style-type: none"> Avoid publishing data from a single facility. If there is a need to release data from a single facility, release visit percentages or rates per 10,000 visits instead of counts. Consult with local health jurisdictions prior to releasing findings related to a specific jurisdiction’s residents. Data provided through RHINO’s drug overdose synopsis dashboard is for internal use only and cannot be used in public facing products. Contact RHINO staff if you need to use this information for any other purpose.

Review Requirements for Peer-Reviewed Publications and Conference Presentations and other Data Releases

- Peer-reviewed publications that include NWTEC staff as co-authors must be reviewed and approved by the Portland Area IHS IRB prior to publication.

- Manuscripts that utilize data stewarded by the IDEA-NW project or the Epidemiology & Surveillance Unit can be submitted through IRBNet under the IDEA-NW project protocol. Contact the IDEA-NW project director if you need assistance with submitting a manuscript.
- Conference presentations that report analytic findings should be submitted to the Portland Area IHS IRB prior to presentation.
 - Presentations can be submitted after an abstract is officially accepted by a conference or meeting.
 - Presentations that utilize data stewarded by the IDEA-NW project or the Epidemiology & Surveillance Unit can be submitted through IRBNet under the IDEA-NW project protocol. Contact the IDEA-NW project director if you need assistance with submitting a presentation.
- Many state data providers require peer-reviewed publications and occasionally other data products be submitted for review prior to publication or public dissemination. The table below summarizes the requirements by data provider.

Data Source/System	Requirements for review and approval
Cancer Data Registry of Idaho (CDRI)	<ul style="list-style-type: none"> ● All manuscripts for publication that make reference to CDRI, or use CDRI data, will be subject to review by CDRI and the Cancer Analysis Work Group. CDRI shall be provided courtesy copies of all final publications.
Idaho Time-Sensitive Emergency Registry (Trauma, Stroke, and STEMI registries)	<ul style="list-style-type: none"> ● All manuscripts for publication that use TSE Registry data will include a TSE Registry staff member as a co-author, provided the TSE Registry staff member abides by International Committee of Medical Journal Editors authorship criteria (http://www.icmje.org/recommendations/browse/roles-and-responsibilities/defining-the-role-of-authors-and-contributors.html). All manuscripts for publication that make reference to the TSE Registry will be subject to review and approval by the TSE Registry. Researchers shall provide the TSE Registry courtesy copies of all final publications.
Idaho Vital Records (births and deaths)	<ul style="list-style-type: none"> ● Provide The Bureau of Vital Records and Health Statistics with review rights – prior to publication – of any document that reports Idaho-specific data. ● Provide to The Bureau of Vital Records and Health Statistics a final copy of any publications, results, reports, etc., derived from the use of the data.
Oregon ALERT Immunization Information System (IIS)	<ul style="list-style-type: none"> ● Any published information that results from linkages with ALERT IIS under this Agreement will be sent to Oregon Immunization Program ALERT IIS staff and to the Indian Health Service Portland Area Office Institutional Review Board for approval prior to publication.
Oregon ESSENCE	<ul style="list-style-type: none"> ● Consult with Oregon ESSENCE before publicly publishing or reporting ESSENCE data.

Oregon State Cancer Registry (OSCaR)	<ul style="list-style-type: none"> Any published information that results from linkages with OSCaR will be sent to OSCaR staff and to the Indian Health Service Portland Area Office Institutional Review Board for approval prior to publication.
Oregon PRAMS	<ul style="list-style-type: none"> Submit the following end products to the PRAMS Coordinator for review by the stated deadlines: <ul style="list-style-type: none"> Manuscripts – submit 28 days before submission Abstracts, oral presentations, poster presentations – submit 14 days before submission/presentation
Oregon Vital Records	<ul style="list-style-type: none"> Notify the Oregon Center for Health Statistics (CHS) of any peer-reviewed journal articles utilizing CHS prior to the data being published
Washington Healthy Youth Survey	<ul style="list-style-type: none"> Submit all copies of reports using Health Youth Survey data to Cathy Wasserman at WADOH
Washington PRAMS	<ul style="list-style-type: none"> Submit copies of reports, press releases, web pages, and any publications of PRAMS data to Linda.Lohdefinck@doh.wa.gov or WAPRAMS@doh.wa.gov
Washington RHINO	<ul style="list-style-type: none"> Submit summaries produced for non-urgent data requests from tribes to the RHINO program for review prior to release to the requestor. Responses to urgent data requests to support immediate public health actions do not need to undergo review from the RHINO program. Submit copies of all papers, presentations, reports, or publications developed using RHINO data to the attention of the RHINO program at rhino@doh.wa.gov

Authorship and Co-Authorship Guidelines

- Authors of peer-reviewed manuscripts and conference abstracts should invite the Principal Investigators overseeing the project and staff involved with data acquisition, quality improvement, and preparation activities to be co-authors on their publications and presentations.
- Authors are responsible for following the authorship and review requirements noted in the [Review Requirements for Peer-Reviewed Publications and Conference Presentations](#) section of this handbook.
- When possible, authors should acknowledge the Northwest Tribes and/or NPAIHB delegates for their support.

Release of data to the media and through social media channels

- Responses to data requests from the media must conform with the requirements and guidelines provided in this handbook and with the media inquiry policy outlined NPAIHB's POM.
 - Employees shall not speak to the media on behalf of the NPAIHB without express approval of the Executive Director. All media inquiries must be directed to the Executive Director.
- Release of aggregated data through social media channels must conform with the requirements and guidelines provided in this handbook and with the Social Media Guidelines outlined in NPAIHB's POM and be approved by the Executive Director prior to release.

Review and updates to this document

The IDEA-NW and Epidemiology and Surveillance Unit project directors will review this document at least annually and revise when needed. The NWTEC Director will approve any substantive additions or changes to this document. Annual reviews and any revisions will be documented in the [Document History](#) section. Items to be addressed in future versions of this document will be documented in the log below.

What is the item or issue that needs to be addressed?	Which section will this be addressed in?	What is the timeline or trigger for addressing?
Document access auditing for server folders that contain PHI/PII (IDEA-NW Data, EDM data folder)	Storage of PHI and Tribal Data on NPAIHB servers (page 13)	Pending discussions with IT department on feasibility of implementing this change
Move PHI/tribal data to encrypted server	Data Storage and Access (pages 12-13), Folder and file organization (page 17)	Pending discussions with IT department on feasibility of implementing this change
Documentation and storage of historical/legacy datasets	Data asset inventory (page 9), Data Storage and Access (page 13)	No set timeline
Expansion of scope to include projects in other Divisions	All sections as needed	Beginning November 2024

Future directions for data governance at NPAIHB

This handbook serves as a starting point for supporting data governance within the NWTEC and NPAIHB. As NPAIHB and its infrastructure, programs, policies, and priorities change, there will be a need for data governance policies and practices to also evolve. Potential future activities to support data governance at NPAIHB include:

- Establishing a cross-departmental data governance committee to lead efforts to develop and implement data governance policies across the organization.
- Assessing training needs and developing training plans to increase awareness and skills in data governance at multiple levels.
- Exploring [participatory data governance frameworks](#) to ensure NPAIHB's member Tribes have opportunities to inform data governance at NPAIHB.

Appendices

Appendix A: Security Requirements

This appendix summarizes general requirements for accessing, storing, transferring, and reporting data obtained from state and federal agencies. Please see specific DSAs for each state system to understand any specific requirements for those systems.

- For limited datasets that include record-level health information
 - Access will be limited to: ^{1,2,3}
 - authorized users within NPAIHB
 - for the least amount of time required to do the work.
 - to the minimum amount of information.
 - with the minimum number of privileges.
 - No record-level data will be re-released to non-NPAIHB staff and approved contractors unless approved by the data provider.
 - Passwords
 - Passwords must be complex and: ^{1,2}
 - At least 8 characters in length.
 - Contain at least three of the following: 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.
 - Changed at least every 90 days.
 - Data Storage
 - 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. ^{1,2,3}
 - Authentication must occur using a unique user ID and Complex Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. ^{1,2,3}
 - Users must utilize multi-factor authentication for accounts with access to data. Accounts must lock after 5 unsuccessful access attempts, after which the accounts will require an administrator reset. ²
 - Methods used to store data must be encrypted using 256-bit Advanced Encryption Standard (AES-256). ^{1,3} Industry standard mechanisms and algorithms, such as those validated by the National Institute of Standards and Technology (NIST) are required. ^{2,3}
 - Data Transfer
 - Methods used to transfer data must be encrypted using AES-256. ³ Industry standard mechanisms and algorithms, such as those validated by the National Institute of Standards and Technology (NIST) are required. ^{2,3}
 - Data Backup

- The data are backed up using a process that includes secure and encrypted storage and transport using the data storage and transfer standards outlined above.^{2,3}
 - Data Segregation
 - The data must be segregated by state and data system/provider, or otherwise distinguishable from all other data. This is to ensure that 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.^{2,3}
 - Additional Considerations
 - Compliance with [HIPAA Security Rule](#) is required for some data provided by IHS.³
 - Authorized users must comply with minimum operating system and software requirements (e.g., encryption and anti-virus utilities), as defined by the NPAIHB's IT department.¹
- For aggregated data released through data products, the Data Hub, and other means:
 - Access to Tribe-specific (or Tribal area-specific) data will only be provided to authorized persons within the Tribe, or persons designated by the tribe to receive access.¹
 - Data cannot be released at a level that could potentially identify an individual (i.e., requires aggregation to meet reporting thresholds).^{1,2,3}
 - Data must be released in accordance with the suppression guidelines outlined in the [Small Numbers and Data Suppression](#) guidelines in this document.

References:

1. NWTEC Data Governance Handbook
2. Idaho, Oregon, and Washington state data sharing agreements
3. Indian Health Service data sharing and rules of behavior agreements for Epi Data Mart Data

Appendix B: Instructions for accessing the CITI Human Subjects Training Course

- 1) Click on this link: <https://about.citiprogram.org/organizational-learners/>
- 2) Under the box titled “Take Courses Assigned by Your Organization”, click the hyperlinked text “register now” in the sentence: You can [register now](#) to take CITI Program content assigned to you by your organization for no charge.
- 3) On the next page, click “Select Your Organization Affiliation”.
- 4) Enter "Indian Health Service (DHHS) Research Program" in the prompt box.
- 5) Check the "I Agree to the terms of service and Privacy Policy," box.
- 6) Check the "I affirm that I am an affiliate of the Indian Health Service (DHHS) Research Program," box.
- 7) Follow the remaining prompts to set up your account and access the training.

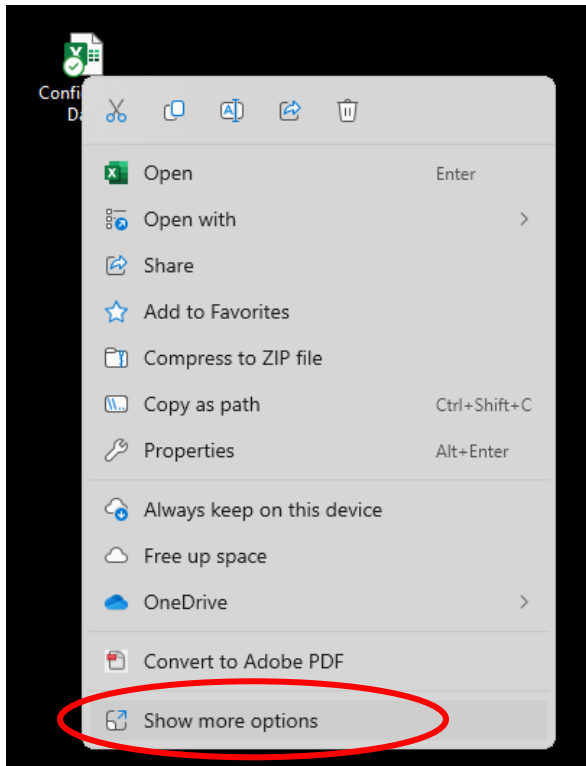
Appendix C: How to securely shred files

Currently, NPAIHB staff can use the secure shred function in the AVG Business software to permanently destroy files. Note that AVG Business was uninstalled on most NPAIHB computers in November/December 2023, but NPAIHB’s IT department can reinstall this program upon request.

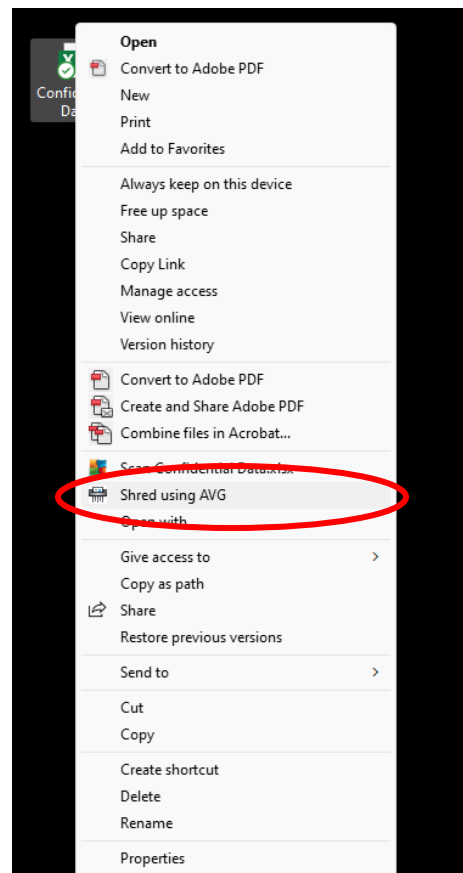
Files that are securely shredded cannot be recovered.

The screenshots below are from a system running Windows 11.

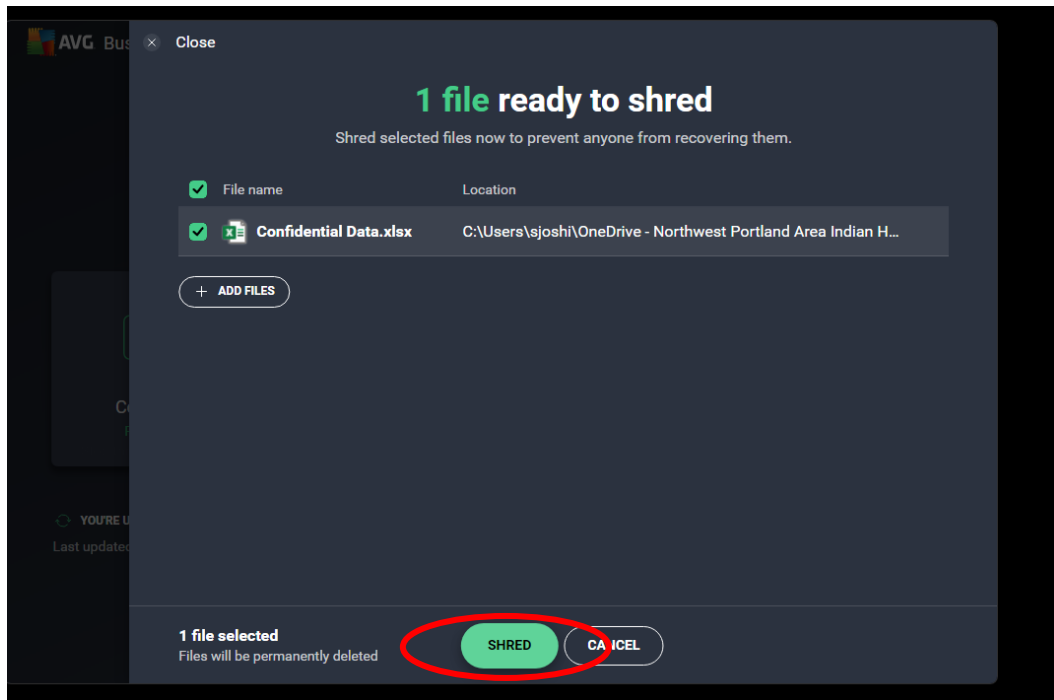
Step 1: Right click on the file you want to destroy and choose “Show more options” (at the bottom of the menu). For earlier versions of Windows, skip this step.



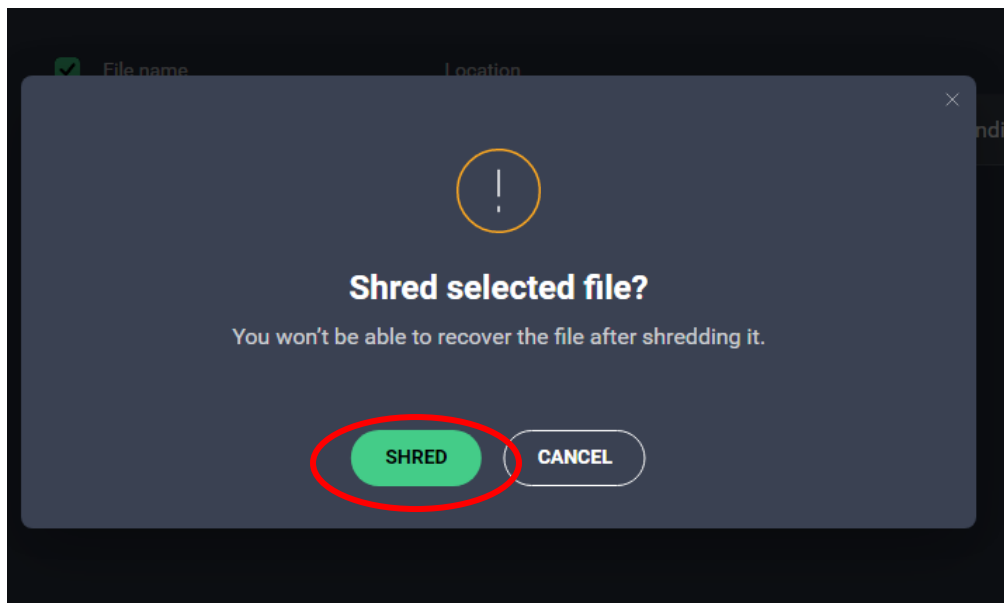
Step 2: Click on the “Shred using AVG” menu option.



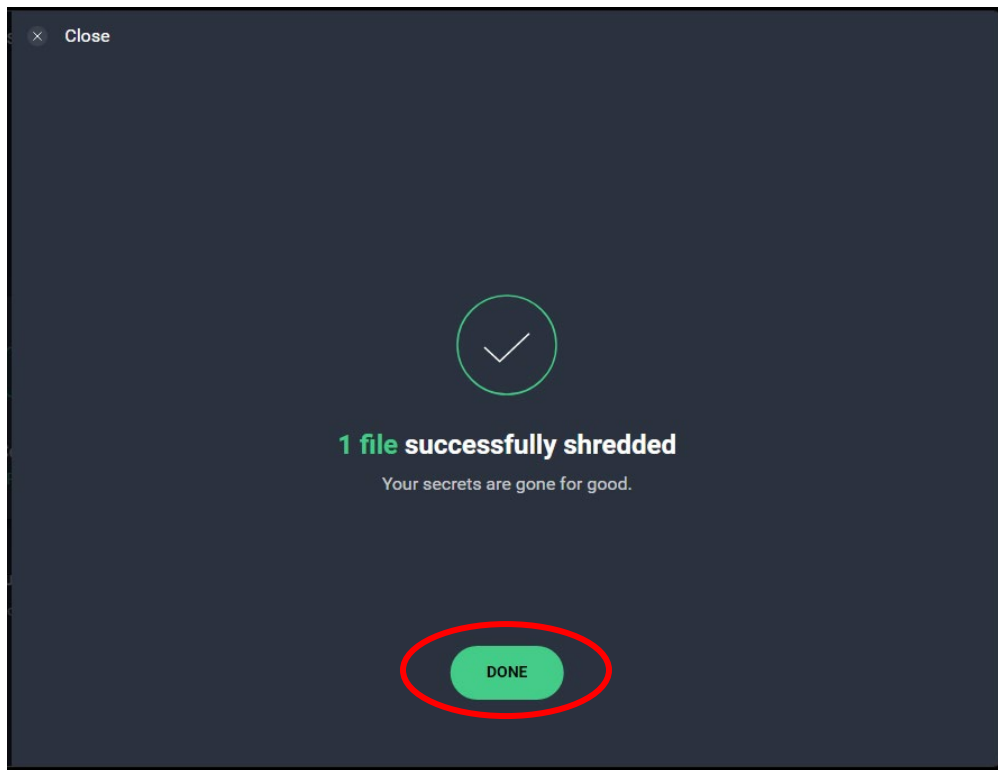
Step 3: A dialog box will open with a list of the file(s) that are selected for shredding. Confirm that the list is correct and click “Shred” at the bottom of the dialog box.



Step 4: A second dialog box will open asking you to confirm that you want to shred the file. Click “Shred”.

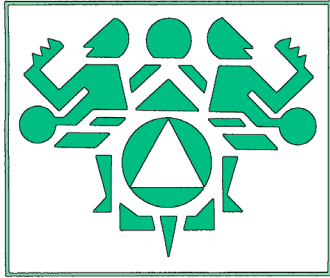


Step 5: A dialog box stating that the shredding is in process will display while the file is being destroyed. When complete, the following dialog box will display. Click “Done”, and then close the remaining dialog boxes.



Appendix E: Templates and other Resources

Template Certificate of Data Destruction



CERTIFICATE OF DATA DESTRUCTION

Northwest Tribal Registry Project/
Improving Data & Enhancing Access (IDEA-NW) Project

Northwest Portland Area Indian Health Board

The undersigned hereby certifies that all copies of the following data files provided to

by _____

on _____ have been destroyed.

Description of files destroyed (e.g., file names, data elements, date range, media storage/file type(s)):

Method of destruction: _____

Date of destruction: _____

Responsible party (print name)

Signature

Date

Appendix F: Definitions

- Aggregated data – data that have been combined and summarized so that individuals can no longer be easily identified.
- Authorized users – individuals who are authorized by NPAIHB to access, use, or disclose confidential data. This may include NPAIHB permanent and temporary employees, contractors, consultants, and other persons or entities.
- Confidential information – information that is protected from public disclosure by law or policy.
- Data governance – the overall management of the availability, usability, integrity, and security of data used in an organization.
- Data sharing agreement – formal contracts between two or more parties that detail what data are being shared, appropriate uses and ownership of data, and restrictions and requirements for data use and release. In this document, the term “data sharing agreement” is used broadly and includes other types of agreements that govern the exchange of data between NWTEC and tribal, state, and federal entities. These types of agreements include data sharing agreements, data use agreements, memoranda of agreement, memoranda or understanding, etc.
- Data breach – an action or event that results in unauthorized access to sensitive or confidential data.
- De-identified data – data in which information that could directly identify an individual (e.g., name, social security number, address, telephone number, account numbers, biometrics) has been removed.
- Encryption – the use of algorithms to encode data making it impossible to read without an encryption key.
- Health information – any information, including genetic information, whether oral or recorded in any form or medium, that:
 1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
 2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.
- Health Insurance Portability and Accountability Act (HIPAA) – legislation passed in 1996 designed to make it easier for workers to retain health insurance coverage when they change or lose their jobs, and also encourages the use of electronic health records to improve healthcare information sharing and quality of care. The HIPAA Privacy Rule and the Health Information Technology for Economic and Clinical Health Act (HITECH) establish standards to protect the security, privacy, and sharing of protected health information.
- Limited dataset – dataset that includes record-level data (i.e.- non-aggregated) that does not include direct identifiers (name, address, social security number, etc.) but does include potentially identifiable information (indirect identifiers, such as gender, race, birth date, geographic location, etc.).

- Personally identifiable information (PII) – any information or combination of information that could directly or indirectly identify the individual to whom the information applies.
- Primary data – data collected first-hand by an organization.
- Protected health information (PHI) – individually identifiable health information that includes demographic information, past, present or future physical or mental health status, and provision or payment of health care. There are federal protections for the use and disclosure of PHI held or transmitted by an entity subject to the HIPAA Privacy Rule.
- Record-level data – data that is specific to an individual, event, or encounter.
- (NPAIHB) Resolution – a document that formally describes the will (i.e., policies, decisions, recommendations) of NPAIHB’s Board of Delegates.
- Restricted access – data storage locations that are only accessible by designated individuals.
- Secondary data – data collected by another entity or for another purpose.

Appendix G: Resolutions and other supporting documentation

Resolution 05-04-04: Tribal Ownership of Data



NORTHWEST PORTLAND AREA INDIAN HEALTH BOARD

Burns Paiute Tribe
Chehalis Tribe
Coquiam Indian Tribe
Colville Tribe
Coos, Siskiyou &
Lower Umpqua Tribe
Coquille Tribe
Cow Creek Tribe
Cowlitz Tribe
Grand Ronde Tribe
Hoh Tribe
Jameson S'Klallam Tribe
Kalapui Tribe
Klamath Tribe
Kootenai Tribe
Lower Klamath Tribe
Lummi Tribe
Makah Tribe
Muckleshoot Tribe
Nez Percé Tribe
Nisqually Tribe
Nooksack Tribe
NW Band of Shoshoni Tribe
Port Gamble S'Klallam Tribe
Pigai Tribe
Quileute Tribe
Quinalt Tribe
Sahish Indian Nation
Santiam Indian Tribe
Shoshone-Bannock Tribe
Siletz Tribe
Skokomish Tribe
Snoqualmie Tribe
Spokane Tribe
Squamish Indian Tribe
Stillequamish Tribe
Squamish Tribe
Swanoma Tribe
Tulalip Tribe
Umatilla Tribe
Upper Skagit Tribe
Warm Springs Tribe
Yakama Nation

527 SW Hall
Suite 300
Portland, OR 97201
☎ (503) 228-4185
FAX (503) 228-8182
www.npaihb.org

RESOLUTION # 05-04-04

Tribal Ownership of Health-Related Data

WHEREAS, the Northwest Portland Area Indian Health Board (NPAIHB) is a tribal organization under P.L. 93-638 that represents forty-three federally-recognized Indian tribes in Oregon, Washington and Idaho and is dedicated to assisting and promoting the health needs and concerns of Indian people in the Northwest, and

WHEREAS, the Northwest Portland Area Indian Health Board is dedicated to assisting and promoting the health needs and concerns of Indian people, and

WHEREAS, the primary goal of the Northwest Portland Area Indian Health Board is to improve the health and quality of life of its member tribes, and

WHEREAS, Northwest Tribes have the right to self-determination, and in exercising that right must be recognized as the exclusive owner of indigenous knowledge, cultural and biogenetic resources, and intellectual property; and

WHEREAS, these elements have been, and continue to be, damaged, destroyed, stolen, and misappropriated, as Tribal members have been the subjects of research for decades, with virtually no benefits returning back to the community from the research; and

WHEREAS, members of the NPAIHB recognize that one way to help safeguard the best interests of Northwest tribal communities is to utilize the Portland Area Indian Health Service Institutional Review Board (PAIHS IRB) to review proposed research protocols and in so doing help prevent research-related abuses of individuals and tribal communities, protect human subjects and traditional knowledge and properties, and to identify research-related benefits and risks to their Tribal communities; and

WHEREAS, members of the NPAIHB recognize that it must: (1) protect the people, culture, and natural resources of the NPAIHB from unauthorized scientific research; (2) reduce the adverse effects of research on Tribal communities; (3) ensure that researchers recognize Tribal control of research activities and Tribal ownership of all data and information generated or produced by such research, and; (4) Establish and provide a statutory basis to review and govern any research, collection, database, or publication undertaken on their Reservations; and

WHEREAS, any tribe that participates in health-related research must be given possession of the primary data (with the necessary protections taken to protect the rights and privacy and confidentiality of individuals).

NOW THEREFORE BE IT RESOLVED, that the Northwest Portland Area Indian Health Board hereby recommends that all health-related research undergo review and approval by the PAIHS-IRB prior to data collection and associated publication of reports; and

BE IT FURTHER RESOLVED that the tribe (and the PAIHS IRB, acting as an agent of the interests of American Indian and Alaska Native people, though not speaking for any individual tribe) have the opportunity to review and give input on publications (and presentations to the extent possible) while they are in draft form (NOT after already submitted to a journal or conference).

BE IT FINALLY RESOLVED, that there will be a formal process by which tribes and tribal organizations will give input as how data concerning their community is presented, and the following principles are adhered to in research projects concerning Northwest Tribal communities:

1. that investigators will not transfer the data to any other party without formal agreement from the tribe (and oversight by the PAIHS IRB, if involved), and
2. that no secondary analyses are performed on the data that are different than those proposed in the original research protocol without a formal request to the affected tribe (and PAIHS IRB, if involved), and
3. that there are measures taken to meaningfully inform the community of the results of research, and
4. that the tribe has the opportunity to benefit from gains that come out of the research (whether that means monetary profits or benefits in terms of better health), and
5. that the tribe has control over how and when data is disposed of (meaning that the storage of data is explicitly laid out, as are the plans for where and when and how it will be destroyed when no longer needed).

CERTIFICATION

NO. 05-04-04

The foregoing resolution was duly adopted at the regular session of the Northwest Portland Area Indian Health Board. A quorum being established; 19 for, 0 against, 0 abstain on July 19th, 2005.

Alan Capanna Feltz
Chairman

July 21st, 2005
Date

Stella M. Washines
Secretary

Resolution 21-04-03: Linkages with the Northwest Tribal Registry



NPAIHB

Member Tribes of
the Northwest
Portland Area
Indian Health
Board:

Bumwilda Tribe
Chehalis Tribe
Coquille Tribe
Cowlitz Tribe
Coos, Siuslaw & Lower
Umpqua Tribe
Cowlitz Tribe
Cove Creek Tribe
Crescent Tribe
Grand Ronde Tribe
Hoh Tribe
Jamezoven S'Kallam
Tribe
Kalispel Tribe
Klamath Tribe
Kootenai Tribe
Lower Elwha
Klallam Tribe
Lummi Tribe
Makah Tribe
Mesa Grande Tribe
Neah-ah-Hale Tribe
Nasqually Tribe
Nasook Tribe
NW Band of
Wasco Tribe
Nasook S'Kallam
Tribe
Puyallup Tribe
Quillayute Tribe
Quinaltup Tribe
Sawtooth Nation
Siletz Tribe
Shooswet Bay Tribe
Shoshone-Bannock
Tribe
Siletz Tribe
Skokomish Tribe
Squamish Tribe
Spokane Tribe
Souxw'isanc Tribe
Streguamish Tribe
Suntamish Tribe
Swinomish Tribe
Tulalip Tribe
Tumwalle Tribe
Upper Skagit Tribe
Warm Springs Tribe
Yakima Nation

2121 SW Broadway
Suite 300
Portland, OR 97201
Phone: (503) 226-4185
npaihb.org

RESOLUTION # 21-04-03

Support for NPAIHB EpiCenter Access and Record Linkages with Public Health Surveillance Systems in Idaho, Oregon, and Washington

WHEREAS, the Northwest Portland Area Indian Health Board (hereinafter "NPAIHB" or "Board") was established in 1972 to assist Tribal governments to improve the health status and quality of life of Indian people; and

WHEREAS, the NPAIHB is a "tribal organization" as defined by the Indian Self-Determination and Education Assistance Act (P.L. 93-638 seq. et al) that represents forty-three federally recognized tribes in the states of Idaho, Oregon, and Washington; and

WHEREAS, in accordance with the definitions of the Indian Self-Determination and Education Assistance Act at 25 USC § 450b, a tribal organization is recognized as a governing body of any Indian tribe and includes any legally established organization of Indians which is controlled, sanctioned, or chartered by such governing body or which is democratically elected by the adult members of the Indian community to be served by such organization and which includes the maximum participation of Indians in all phases of its activities; and

WHEREAS, the NPAIHB is dedicated to assisting and promoting the health needs and concerns of Indian people; and

WHEREAS, the primary goal of the NPAIHB is to improve the health and quality of life of its member Tribes; and

WHEREAS, in furtherance of this goal in 1997, NPAIHB established the Northwest Tribal Epidemiology Center (EpiCenter) in an effort to improve the quality of American Indian and Alaska Native (AI/AN) public health data; and

WHEREAS, the EpiCenter has gained national recognition for developing and implementing many useful and innovative projects to improve the health and quality of life of Northwest Tribes and has served as a national model for other Indian Health Service (IHS) areas to emulate in establishing their epi center programs; and

WHEREAS, with Board approval, the EpiCenter maintains the Northwest Tribal Registry (NTR) to perform record linkage studies to identify and correct racial misclassification in various public health surveillance systems to better assess the health status of Northwest AI/AN people; and

WHEREAS, previous studies by the EpiCenter has shown that morbidity and mortality estimates for Northwest AI/AN people are under-reported due to misclassification of race in public health surveillance systems; and

WHEREAS, AI/AN people in Idaho, Oregon, and Washington experience significant health disparities from many causes; and

WHEREAS, the correct identification of AI/AN in public health data is essential for monitoring tribal communities' health and planning prevention and intervention efforts; and

WHEREAS, the EpiCenter has consistently demonstrated adequate measures to ensure the physical security of data and has policies in place to control access to and release of data; and

WHEREAS, any dissemination of results to outside audiences will only be done in collaboration with and by approval of NPAIHB, the EpiCenter, the Portland Area IHS Institutional Review Board, and member tribes.

THEREFORE BE IT RESOLVED, that the NPAIHB endorses and supports efforts by staff of the EpiCenter, under the guidance of the Executive Director, to access, and when possible, complete record linkages with the following public health surveillance systems in Idaho, Oregon, and Washington to correct racial misclassification of AI/AN people and more accurately report health status data for AI/AN people in the Northwest:

- Vital records data, including birth and death records
- Hospital and emergency department surveillance and reporting systems
- Notifiable conditions surveillance systems, including but not limited to COVID-19, HIV, sexually transmitted infections, and Hepatitis B and C surveillance systems
- Disease registries, including but not limited to cancer, trauma, blood lead, stroke, and STEMI registries
- Medicaid claims data
- Prescription Drug Monitoring Program data
- Emergency Medical Services data
- Fatality Analysis Reporting and Motor Vehicle Accident reporting systems
- Violent Death Reporting System data
- Pregnancy Risk Assessment Monitoring System (PRAMS) data
- Adult and youth risk factor surveillance systems

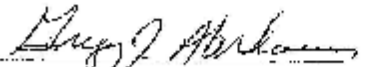
CERTIFICATION

The foregoing resolution was adopted by the Board of Directors at the Quarterly Board Meeting, held virtually July 27 – 29, 2021, with a quorum present.



Nickolaus D. Lewis
Chair, Northwest Portland Area Indian Health Board
Councilman, Lummi Indian Business Council

ATTEST:


Greg Abrahamson, NPAIHB Secretary

Resolution 21-04-04: NDW Access for Record Linkages



NPAIHB

Member Tribes of
the Northwest
Portland Area
Indian Health
Board:

Bumwautuck Tribe
Chehalis Tribe
Coquille Tribe
Cowlitz Tribe
Coos, Siuslaw & Lower
Umpqua Tribe
Cowlitz Tribe
Cove Creek Tribe
Creswell Tribe
Grand Ronde Tribe
Hoh Tribe
Jamezoven S'Kallam
Tribe
Kalispel Tribe
Klamath Tribe
Kootenai Tribe
Lower Elwha
Klallam Tribe
Lummi Tribe
Miyam Tribe
Muckleshoot Tribe
Neah-ah-Hale Tribe
Nasqually Tribe
Nooksack Tribe
NW Band of
Wasco Tribe
Naselle S'Kallam
Tribe
Puyallup Tribe
Quiltsat Tribe
Quinalt Tribe
Sawtooth Indian Nation
Siletz Tribe
Sho-wah-Be Tribe
Shoshone-Bannock
Tribe
Siletz Tribe
Skokomish Tribe
Snoqualmie Tribe
Spokane Tribe
Souxw'isanc Tribe
Stillequamish Tribe
Suntamish Tribe
Swinomish Tribe
Tulalip Tribe
Tumwalle Tribe
Upper Skagit Tribe
Warm Springs Tribe
Yakima Nation

2121 SW Broadway
Suite 300
Portland, OR 97201
Phone: (503) 226-4185
npaihb.org

RESOLUTION # 21-04-04

Support for NPAIHB EpiCenter Access to the Indian Health Service's National Data Warehouse Data for Record Linkages

WHEREAS, the Northwest Portland Area Indian Health Board (hereinafter "NPAIHB" or "Board") was established in 1972 to assist Tribal governments to improve the health status and quality of life of Indian people; and

WHEREAS, the NPAIHB is a "tribal organization" as defined by the Indian Self-Determination and Education Assistance Act (P.L. 93-638 seq. et al) that represents forty-three federally recognized tribes in the states of Idaho, Oregon, and Washington; and

WHEREAS, in accordance with the definitions of the Indian Self-Determination and Education Assistance Act at 25 USC § 450b, a tribal organization is recognized as a governing body of any Indian tribe and includes any legally established organization of Indians which is controlled, sanctioned, or chartered by such governing body or which is democratically elected by the adult members of the Indian community to be served by such organization and which includes the maximum participation of Indians in all phases of its activities; and

WHEREAS, the NPAIHB is dedicated to assisting and promoting the health needs and concerns of Indian people; and

WHEREAS, the primary goal of the NPAIHB is to improve the health and quality of life of its member Tribes; and

WHEREAS, in furtherance of this goal in 1997, NPAIHB established the Northwest Tribal Epidemiology Center (EpiCenter) in an effort to improve the quality of American Indian and Alaska Native (AI/AN) epidemiology data; and

WHEREAS, the EpiCenter has gained national recognition for developing and implementing many useful and innovative projects to improve the health and quality of life of Northwest Tribes and has served as a national model for other Indian Health Service (IHS) areas to emulate in establishing their EpiCenter programs; and

WHEREAS, Section 214 of the Indian Health Care Improvement Act (P.L. 110-148) amends current law to continue authority for operation and funding of Tribal Epidemiology Centers and gives epi centers the status of public health authorities for purposes of the Health Insurance Portability and Accountability Act of 1996, thus granting access to health data needed to perform their mission; and

WHEREAS, the correct identification of AI/AN people in surveillance and health claims data systems is essential for understanding the burden and distribution of disease, mortality, and health care utilization for public health planning; and

WHEREAS, previous studies by the EpiCenter have shown that public health data for Northwest AI/AN people are under-reported due primarily to misclassification of race in public health registries and vital health records; and

WHEREAS, the EpiCenter has, with Board approval, used the Northwest Tribal Registry (NTR) to conduct record linkages to identify and correct racial misclassification in various public health registries to better assess burden of disease for Northwest AI/AN people; and

WHEREAS, the most comprehensive listing of AI/AN people in the Northwest is the IHS National Data Warehouse; and

WHEREAS, to have the capability to perform ongoing projects that improve the quality and accessibility of health data for Northwest Tribes (for example, record linkages with cancer registries, vital statistics, hospital and emergency department data systems, trauma registries, and STD/HIV registries), the EpiCenter needs ongoing access to the IHS National Data Warehouse; and

WHEREAS, the EpiCenter has consistently demonstrated adequate measures to ensure the physical security of data and has policies in place to control access to and release of data; and

WHEREAS, any dissemination of results to outside audiences will only be done in collaboration with and by approval of NPAIHB, the EpiCenter, the Portland Area IHS Institutional Review Board, and member tribes.

THEREFORE BE IT RESOLVED, that the NPAIHB requests the support of the Portland Area IHS Office and the National Office of the Indian Health Service (IHS) to provide the EpiCenter with National Data Warehouse data annually for the purposes of updating the Northwest Tribal Registry.


CERTIFICATION

The foregoing resolution was adopted by the Board of Directors at the Quarterly Board Meeting, held virtually July 27 – 29, 2021, with a quorum present.



Nickolaus D. Lewis
Chair, Northwest Portland Area Indian Health Board
Councilman, Lummi Indian Business Council

ATTEST:



Greg Abrahamson, NPAIHB Secretary

NWTEC Strategic Framework for Data Modernization



**NORTHWEST PORTLAND AREA
INDIAN HEALTH BOARD**
Indian Leadership for Indian Health

Strategic Framework for Data Modernization

Vision Statement

Our shared vision for EpiCenter data modernization is to provide high-quality* public health data and support for Northwest Tribes to promote healthy tribal communities.

*accurate, complete, reliable, relevant, timely

Value Statements

Data Sovereignty

We believe in the rights of tribes to define data and populations of focus, and govern the collection, ownership, and application of their own data.

Capacity Building

We believe in building the knowledge, techniques, and skills of individuals and cultivating effective and enabling institutions (i.e., NPAIHB, Board staff, Board delegates, Member Tribes institutions and staff)

Sustainability

We believe in efficient and impactful use of resources for successful, long-term data modernization

Attributes of a Future State

Efficient data collection and transformation

Enhanced data discovery

Appropriately accessible data and analysis

Coordinated data modernization activities across EpiCenter programs and projects with tribal, state, and federal partners

Strategies

A. Coordinate initiatives, funding, and opportunities internally (i.e., the EpiCenter, the Board)

B. Improve data collection, transformation, and management processes to enable efficient data discovery and use

C. Expand customized data analysis for internal and external partners

D. Identify and invest in a core set of robust and cost-efficient tools for data analysis and visualization for use across the organization

E. Centralize data activities (collection, management, and analysis) in a shared services office

F. Coordinate initiatives, funding, and opportunities externally (i.e., Member Tribes, state and federal partners)