NORTHWEST TRIBAL DATA HUB

Data Security Fact Sheet

The Northwest Tribal Data Hub (Data Hub), developed by the Northwest Portland Area Indian Health Board (NPAIHB), provides secure access to public health data for Tribes in Idaho, Oregon, and Washington through interactive dashboards. The NPAIHB ensures Tribal Data Sovereignty through robust data protection. The Data Hub, hosted on Amazon Web Services (AWS), uses multiple layers of security managed by AWS, NPAIHB, and Tribes.

PROTECTING TRIBAL DATA

Architecture

Defines all the places in a cloud ecosystem that security controls need to be considered.

- The main ways we protect data is through **encryption and access management**, regardless of whether the data is in the database ('at rest') or being uploaded or moved ('in motion').
- The Data Hub's architecture protects data from unwanted access or accidentally exposed to unauthorized users.

Access

Access refers to which individuals and applications have access to any given data.

- Security control to enforce access are accounts (logins) and authentication codes (passwords). We created a security groups model that allows appropriate access to users based on their security group.
- Our Access Security Model protects Tribal data from being shared with the wrong internal/external viewer.

Who has access?

Tribal leadership completes an agreement with NPAIHB and designates an Authorizing Official.

- The Tribe's Authorizing Official designates individuals to access the Data Hub.
- Designated individuals must complete user agreements to access the Data Hub Dashboard.
- Each Tribe can access only their Tribal Area data and aggregate state and regional data.

Data Hub Security Architecture

Physical Protections

- Data is stored in AWS Data Centers with 24/7 security measures including encryption, restricted access, monitoring, and backup power.
- Data backups are maintained on-site, at NWTEC, and in the AWS cloud.

Administrative Protections

- Complex passwords for user logins.
- Access to Tribal-specific data is restricted.
- Only NWTEC Data Hub staff and authorized Tribe members can access specific Tribal data.
- Secure access portals for individual logins with activity monitoring.
- Data is de-identified & aggregated for confidentiality.
- Small number standards to prevent identification.

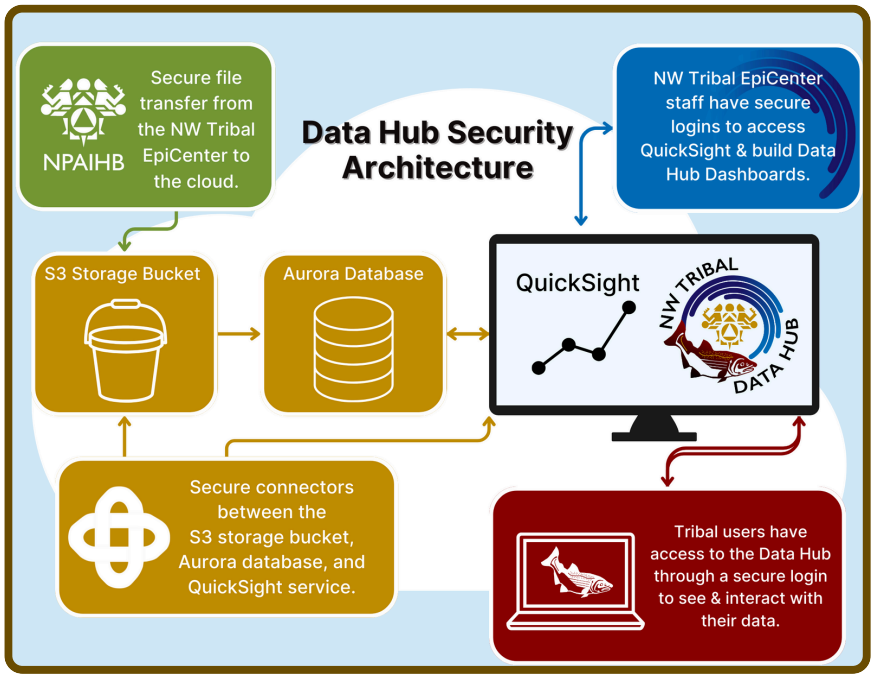
Technical Protections

- Virtual Private Computing and network security.
- Firewalls & no public database access.
- Identity & Access Management (IAM) technology.
- FedRAMP and HIPAA-certified technology.
- Data encryption at rest and in motion with AES-256.
- Multifactor authentication & Virtual Private Network use for NWTEC staff.

What happens if there is a data breach?

In the event of unauthorized access:

- Data Owners, NWTEC, NPAIHB IT, and Executive Directors will be notified.
- If related to a cyber attack, NPAIHB will coordinate with public safety and legal personnel as appropriate.
- All actions will be documented.



For questions, contact the team at datahub@npaihb.org.

This publication and the NW Tribal Data Hub were developed with funding support from the Centers for Disease Control and Prevention (Cooperative Agreement Numbers NU58DP007226 and NU38OT000255) and the Indian Health Service (Cooperative Agreement Number U1B1IHS0004). Its contents and solely the responsibility of the authors and do not necessarily represent the official views of the CDC, IHS, or the U.S. Department of Health and Human Services.