

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 ID, OR, and WA through interactive dashboards. NPAIHB ensures Tribal Data Sovereignty through robust data protection. The Data Hub safeguards Tribal data sovereignty through multiple layers of security and robust data protections.

PROTECTING TRIBAL DATA

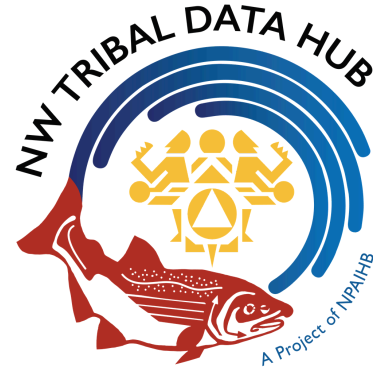
Architecture

Architecture is the blueprint that dictates how the Data Hub is built. It defines how the rooms (services, like the database), hallways (networks), locks (security controls), and utilities (storage and computing) are arranged so the whole system is safe, reliable, cost-efficient, and easy to use. This multi-layered design protects the privacy, security, and availability.

Identity and Access Management (IAM)

IAM refers to the management of users and their privileges within a system. Our role-based security model ensures users have access only to approved resources and data.

- All users are authenticated through trusted identity providers with enforced Multi-Factor Authentication (MFA). Passwords are not stored or managed in the Data Hub.
- Data are protected by security rules restricting access at the record level to approved users.



How can I help to protect my data?

Individual users can protect the security of the Data Hub by following Tribal security policies, the Terms of Use, and following guidelines:

- Only access the Data Hub from private, secure connections, not open public internet networks (like a coffee shop). Virtual private network (VPN) connections are recommended.
- Ensure your screen is not visible to others who do not have the Tribe's permission to access the Data Hub.
- When you have completed your session, log out.
- Protect the device used for MFA with strong passwords and/or biometric authentication.
- Protect dashboard PDF downloads as you would sensitive information.

Data Hub Security Architecture

Data Protections

- Data are stored in a Virtual Private Cloud with no public access.
- Data in the cloud are encrypted using secure NIST-approved AES-256 encryption algorithms in the database and when data are uploaded to cloud storage.
- Encryption keys are securely stored, strongly protected, and automatically rotated.
- Data access is restricted and controlled through identity and access management.
- Individual privacy is protected by presenting only de-identified and aggregated (grouped) data.

Physical Protections

- The cloud provider maintains 24/7 security measures including surveillance, biometric controls, security updates, and physical hardware maintenance.
- Automated backup and disaster recovery.

Cloud Infrastructure Protections

- Strict network controls and firewall protections.
- Automated monitoring and logging.
- HIPAA-compliant services.
- Enforced Virtual Private Network use for NWTEC staff.

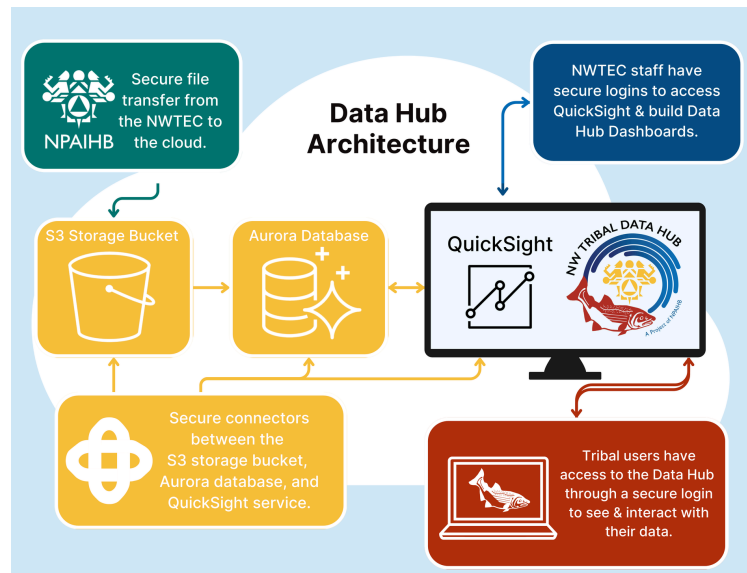
Who has access

- Tribes determine who has access to their Data Hub dashboards. For more information see the Access Fact Sheet.

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.

10001
0101000010101
01010101001001010
10100101110001010100
1010101010010010101110