NativeDATA

A Data Sharing Resource for Native Peoples and Organizations

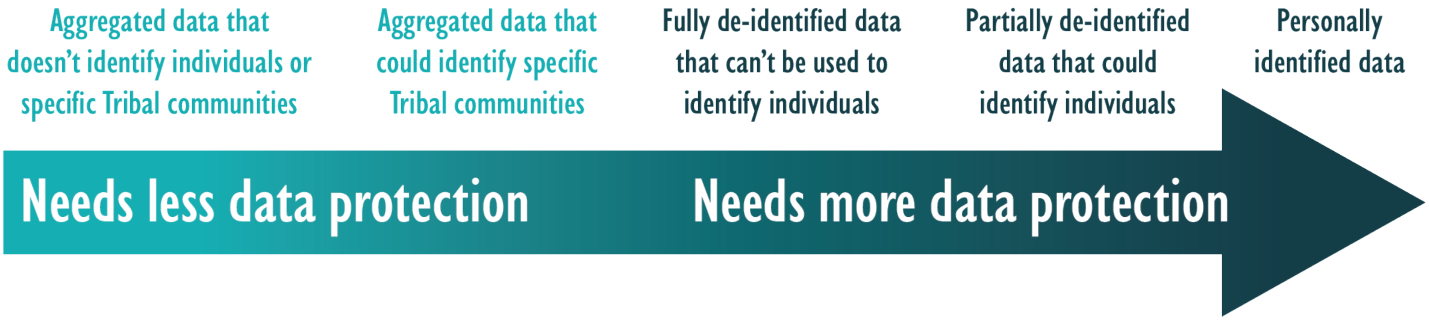
Data Protection and Stewardship

When we work with health data, we must protect the people and communities whose information is contained in it. Data stewardship includes the actions we take to protect data. Data stewardship is important at every stage of working with data. These stages include obtaining, sharing, storing, analyzing, reporting, and destroying data.

Below are some tips for good data stewardship.

Understand what level of protection the data requires.

Different types of data require different levels of protection. Data that are aggregated (or grouped together so that individuals can't be identified) often need less protection than data that could identify an individual. The figure below shows levels of protection that may be needed for different types of data.



Aggregated data that doesn't identify individuals or specific Tribal communities

Aggregated data that could identify specific Tribal communities

Fully de-identified data that can't be used to identify individuals

Partially de-identified data that could identify individuals

Personally identified data

Needs less data protection

Needs more data protection

If you are obtaining data from a local, state, or federal health department, ask what their requirements are for protecting the data you are requesting. Often, a data agreement will list the protections you need at the different stages of working with the data.

Work with the minimum amount of data you need to accomplish your goals.

It can be tempting to request more data than you need to accomplish your goals. However, the more data you have, the more protections you may need to put in place. Work to clearly define the purpose and scope of your data request, and only request the data variables (data measurements) you need to meet that purpose. This worksheet can help you define the purpose, scope, and data variables needed for your request.

Keep in mind

When you request to obtain data, you may be able to ask for different kinds of access. "Live access" means you get to directly access the database and obtain new data as needed. "Static access" means you get a "snapshot" of the data from the database at one point in time. The requirements for data stewardship may be different for "live access" versus "static access".

Use multiple approaches for protecting data.

Data security and protection involves multiple approaches.
These approaches include:

Physical protections

- Keep servers, computers, flash drives, paper files, and other media that store data in locked and secured areas.
- Make sure only people with permission to access data can access these secured areas.

Administrative protections

- Limit the number of people who have access to the data.
- Have a system that keeps a detailed record of who logged in to access the data, when they accessed the data, and what they did. Registering and logging data access are important for ensuring that data are used in ways that are in accordance with your Tribal or organizational data stewardship policies (and any data agreements).
- Make sure people who have access to data understand the reasons and requirements for protecting data. This can be done through information security awareness trainings, privacy trainings, and confidentiality agreements.
- Make sure people who have access to data follow password requirements to access the data. These requirements can include the use of complex passwords, as well as agreements to not share passwords with other people.
- Have written policies and procedures in place that detail how your Tribe or organization manages data in general.
- Have written policies and procedures in place to respond to a loss or breach of data, or a violation of data security requirements.
- Have written confidentiality and/or non-disclosure policies in place for protecting individuals and communities when reporting aggregated data. For example, to protect the privacy of community members in a health report released to the public, only report data when there are more than 5 or 10 cases of a specific health condition. Similarly, Tribal organizations, Tribal Epidemiology Centers (TECs), and other entities should only share data on a specific Tribal community with permission from authorized officials from that Tribal community.

Technical protections

- Make sure hard drives, laptops, flash drives, and other portable media that store data are encrypted at or above appropriate standards. The process of encryption simply means changing data into a secret code to try to prevent those who are unauthorized from reading it.
- Make sure server folders that store data are restricted only to the people with permission to access the data.
- Make sure server folders that store data can only be accessed with appropriate user IDs and passwords or other strong user authentication.
- Make sure you transfer data using a secure method, such as a secure file transfer service.
- When you've finished working with the data, make sure it is completely destroyed if destruction is required in your data agreement.

Work with your Information Technology (IT) team.

Your IT team can help with technical protections such as encryption and server access. They can also:

- Help you with staff training on information security awareness
- Brainstorm with you about possible challenges to sharing or obtaining data
- Develop back-up plans and strategies for overcoming challenges

Make data stewardship an ongoing part of your work.

Data stewardship is an ongoing process. From the time you obtain data to the time you destroy it, make sure everyone with access to data follows the requirements for using the data. Hold annual trainings for staff (and mandatory training for new personnel) to review the importance of protecting data, and the approaches they should take to protect data. Work with your IT team to conduct regular audits of technical protections for data. And review and update any policies you have for data stewardship on a regular basis.

Keep in mind

Staff may need to adjust their data stewardship process based on challenges that arise. Build additional time into your project timeline to accommodate this.

Got Questions?

Consider connecting with one of these data supports.

NPAIHB
NativeDATA

Got questions? Contact us at ideanw@npaihb.org or visit NativeDATA.npaihb.org.

Funding for this resource was generously provided by the Centers for Disease Control and Prevention under a contract from the National Association of County and City Health Officials (CDC cooperative agreement number 6NU38OT000306-02-01).