3.1: Understanding Data Ownership

Data ownership is a relatively new concept in the world of data systems. Ownership typically means having legal title to a piece of property like a house or car. When using this definition, ownership can sometimes be unclear when dealing with digital property like data.

Commonly, a data owner is a person or organization with **the legal right and ability to create, alter, share, or restrict any piece or set of data**. Data owners can assign these functions and responsibilities to other parties (e.g., a system provider) to act on their behalf. These providers host data systems to store and process the data and often have the same capabilities as the owner to edit, share, or restrict data.

Data ownership considerations are critical for all agencies and, in particular, tribal nations who are committed to maintain the sovereign ownership of information on their citizens. Some tribal nations or agencies have clearly defined protocols and requirements for maintaining data ownership, while for others it is left to the agencies to understand and negotiate these issues on a case-by-case basis.

Data Ownership Agreements and Governance

When working with a third-party provider such as a developer or system vendor, your agency has user agreements to define the details of data ownership. Sometimes, separate data ownership agreements are used in addition to any other contracts in place. This agreement lists the agency rights as the owner of the data and defines what access and responsibilities the provider has. The user agreement specifies the policies and responsibilities of the provider. Many agencies find it helpful to define a comprehensive process detailing how they manage, monitor, and maintain their data. This is called **data governance**. A fully documented data governance process establishes control and accountability over agency data, which can be helpful in clarifying data ownership. Your team should check with your tribal or agency attorneys and leadership to determine if any existing agreements, policies, or data governance plans are in place and ensure they are followed.

Clear data ownership policies can be established in the beginning of your work with a vendor so don't forget to check out Module 1 for information on developing Requests for Proposal and choosing a system vendor.

Data Ownership – Core Elements

When developing data ownership agreements or an agency data governance plan, understanding the core elements of data ownership and the considerations related to the five elements listed below are critical.

- **Data Management**. A data management plan describes how data is handled and who has access. This includes specifying whether systems are in place to recover data in the event of loss. The plan also details what access controls are in place, so agency data is only viewed by authorized users.

  Considerations: What happens to data when deleted? Can it be recovered? How is the agency data maintained and by whom?

- **Data Location.** Service agreements from providers who work with government agencies usually specify the location of their data servers. Many government agencies require their data to be physically processed and stored only within the United States.

  Considerations: What is the physical location of the data, and how is it stored? Some agencies may have policy or legal limitations on where certain data may be physically stored.

- **Data Access.** Access defines which personnel/positions may access the agency data and under what circumstances. A service agreement states the provider will have access as necessary to provide services such as developing, maintaining, or changing the system. Most services also offer either an audit tool or report for the agency to track what users have accessed the data.

  Considerations: Who has access to agency data? Can it be accessed outside of the agency; if so, under what circumstances? Is there an audit feature to track who has accessed data and when?

- **Data Privacy/Confidentiality.** A privacy/confidentiality clause describes how the provider will maintain the integrity and security of data. Providers commonly use encryption to secure the data itself along with secure methods to authenticate users so only authorized people can access the system.

  Considerations: What steps are taken to ensure agency data is secure?

- **Data Rights and Retention.** Rights and retention clauses will explain what happens to data when the agreement with the provider comes to an end. Most service providers offer a specified grace period for the agency to retrieve data after the service ends.

  Considerations: What happens to agency data if the relationship with the provider ends? Does the agency retain ownership of any data? Are they destroyed by the vender once the agency has moved to another data system?