IES Institute of Education Sciences

SLDS Record Retention and Data Destruction

SLDS Guide

Statewide Longitudinal Data Systems Grant Program

May 2021

U.S. DEPARTMENT OF EDUCATION

A Publication of the National Center for Education Statistics at IES

Contents

This product of the Institute of Education Sciences (IES) Statewide Longitudinal Data Systems (SLDS) Grant Program was developed with the help of knowledgeable staff from state education agencies and partner organizations. The information presented does not necessarily represent the opinions of the IES SLDS Grant Program.

For more information on the IES SLDS Grant Program or for support with system development, please visit *http://nces.ed.gov/programs/SLDS*.

CONTRIBUTORS
Sean Cottrell and Bill Hurwitch, *SLDS Grant Program State Support Team*
Ross Lemke and Mike Tassey, *Privacy Technical Assistance Center*

Introduction

Statewide longitudinal data systems (SLDSs) contain large amounts of data gathered about individuals over an extended period of time, some of which are personal and may be sensitive. As part of their overall data governance and use strategies, SLDS programs must determine how and how long to keep individual data records in their systems as well as how to safely and securely destroy data that are no longer needed.

Record retention refers to the practices around storing data after they are collected. Retention policies detail how long data records should be stored, where, and in what format. Retention periods may be based on state or agency archiving requirements as well as when specific data need to be used or reported.

Data destruction is the process of eliminating data records that no longer need to be retained. Beyond simply deleting data files from a hard drive or database, secure data destruction practices ensure that the data cannot be recovered. Proper data destruction becomes more complicated when data are stored in multiple places, shared via email, or hosted in cloud or other storage services controlled by third-party providers.

Record retention and data destruction policies often are essential parts of agreements allowing researchers to use SLDS data for studies and analysis. They also have become increasingly important as schools expand their use of classroom technology that collects student information. Well-crafted policies help ensure that SLDS programs manage their data appropriately without trusting solely to data users and partners to store and dispose of data as required.

SLDS programs may have multiple layers of record retention and data destruction policies that apply to different types of data and different situations, such as data used internally by SLDS staff members or data shared with researchers outside the program. This guide discusses considerations that SLDS programs should make when crafting their policies and shares some characteristics of effective policies. It also covers common challenges related to record retention and data destruction that policies should address.

Considerations for Developing Record Retention and Data Destruction Policies

Record retention and data destruction practices for SLDS programs are shaped by a number of factors, including legal requirements, established policies, industry norms, and characteristics of the data system and its data collections. It is important to take all of these factors into account when developing retention and destruction policies.

Methods of data destruction

Data can be destroyed by a variety of means depending how they are stored. Data destruction policies might prescribe any of the following destruction methods.

Clearing: Removing data through software, such as by overwriting the data or "formatting" an entire partition or disk.

Purging: Removing data through physical or logical means, such as applying strong magnetic fields to a disk to reduce the magnetic signature used to store data.

Destroying: Rendering the medium used to store the data unusable, typically through pulverizing, incinerating, or shredding it.

Encryption: Using algorithms to obfuscate data when complete removal or destruction is not possible and then destroying the algorithm.

Federal requirements

The Family Educational Rights and Privacy Act (FERPA), which applies to data from education agencies and programs, has few provisions related to record retention and data destruction. FERPA prohibits schools from destroying data if there is a pending request from a parent or eligible student to access those data. If personally identifiable information about students is shared outside the school as permitted by FERPA's studies or audit or evaluation exceptions, FERPA requires that information to be destroyed when no longer needed for the authorized purpose. Education agencies must establish a written agreement with the organization conducting the study, audit, or evaluation that specifies a time period for data destruction.

In addition to FERPA, some types of data—such as special education data—may be subject to other federal requirements that must be considered when determining how to retain or destroy records.

State laws and IT policies

SLDS programs also must adhere to state laws and policies around record retention and data destruction. Some states require public agencies to retain data about an individual for a specific time period after that individual has graduated or left a program or after the data are no longer needed. Information technology (IT) offices might have additional guidelines for how

long state agencies must retain data, how data are stored, and methods for destroying data. These laws and policies can vary for different types of data and in situations where data must be kept for audits or reporting purposes.

Storage methods

The capacity and type of the SLDS's data storage infrastructure, including whether data are stored electronically or as paper records, may influence how long records are retained and how data that are no longer needed will be destroyed. Record retention policies may need to address whether and how data will be migrated from one system to another if the SLDS's technical structure changes.

Privacy and security best practices

Record retention and data destruction policies should aim to preserve data that the agency needs and securely destroy data that are not essential. Retention and destruction practices will vary for different types of data in the SLDS. The following steps can help SLDS programs categorize their data and create policies that address each type:

- *Perform a data inventory*. For each data element in the SLDS, determine where the element is stored, who owns it, and how sensitive it would be if disclosed.
- *Match the data to business needs*. Identify why the SLDS program collects each data element and how it is used.
- *Convene stakeholders to determine retention needs*. Work with data owners and users to figure out how long to keep each type of data.

These considerations should inform retention criteria and destruction controls targeted to each type of data in the SLDS.

Additionally, SLDS programs should perform a risk analysis to identify threats to different types of data and the consequences of a security breach.

Special considerations for P-20W+ SLDSs

P-20W+ SLDSs contain data from multiple state agencies and programs, often including early childhood care and education, K12 and postsecondary education, workforce programs, and additional state services. Record retention and data destruction policies for a P-20W+ SLDS need to account for the laws and policies governing each of its data sources, such as FERPA for K12 data, as well as how those data are held, managed, and used by organizations that are not usually subject to the same requirements.

Data destruction in cloud-based data systems

Storing data in a cloud environment rather than in on-premises servers controlled directly by a state agency presents unique challenges for data destruction. When creating a data destruction policy, consider how your SLDS program will address the following issues common with cloud-based systems:

- *Shared resources*. Options for destroying data may be limited by where and how they are stored, as well as who controls the storage infrastructure.
- *Distributed architecture*. Because cloud-based systems often store data across multiple locations, the data that you wish to destroy may not exist in a single place.
- *Compliance with security requirements*. Work with vendors to address FERPA and other security regulations, and draft written agreements that clearly address what must happen to data once the project for which they were shared is complete.
- *Confirming data destruction*. What assurances will you have from cloud service providers that data have been destroyed?

What Should Record Retention and Data Destruction Policies Look Like?

No two SLDS programs will have identical record retention and data destruction policies, but comprehensive and actionable policies often do the following.

Separate record retention and data destruction practices

Record retention and data destruction frequently are covered by two distinct policies reflecting the processes, considerations, and individuals involved in each area.

Address different types of data and situations

Record retention and data destruction policies outline multiple sets of procedures for different types of data, such as data covered by FERPA, special education data, and data used by researchers.

Provide comprehensive guidance throughout the data life cycle

Record retention policies define retention periods for different types of data and how they will be stored

as long as they remain in the SLDS. Data destruction policies define acceptable methods of destroying data when they are no longer needed.

Follow best practices for written agreements

Organizations that share data with an SLDS or that use SLDS data must sign written agreements that make clear how those data will be handled and used. Written agreements should comply with federal and state laws for sharing data across agencies or organizations, storing data securely, and destroying the data when the agreement expires.

Outline steps for certifying data destruction

Data destruction policies should specify when and in what method data will be destroyed when they are no longer needed.

Common Challenges for Record Retention and Data Destruction

Comprehensive record retention and data destruction policies help guide SLDS team members in responding to data management, privacy, and security challenges. When developing policies, consider how they address or may be modified to address situations like the following.

Confirming data destruction

In connection with written data sharing agreements, many SLDS programs require researchers or other data users to sign a certificate of data destruction once their studies are complete. Determine whether your program can or should take additional steps to verify that users have appropriately destroyed SLDS data as required. Additionally, consider how to address data that may be saved in email accounts, on backup or personal drives, in the cloud, or in distributed data systems that store data in more than one place.

Responding to an audit

SLDS programs may be subject to federal or state audits to confirm that they are following data privacy and security requirements. Be prepared to demonstrate to auditors that the program complies with record retention and data destruction policies, whether they are statewide or agency specific. SLDS programs can demonstrate compliance using artifacts such as data destruction certificates, minutes from risk management board meetings, vulnerability scanning program metrics, and security controls programmed into data system-related applications.

Additionally, program leaders should be able to answer the following questions related to record retention and data destruction:

- How long are data retained?
- How often are retention schedules reviewed?
- Do you audit to ensure compliance with data destruction and retention policies?

Offering secure, remote access to SLDS data

Many SLDS programs have begun exploring ways to share SLDS data with researchers or other users without making those users responsible for storing or destroying the data at the end of their projects. SLDS programs may require researchers to come to a state-owned facility to view and work with data within the state's IT environment. Some programs are developing cloud-based environments to allow researchers remote access to approved SLDS data while still adhering to all applicable privacy and security policies.

Conclusion

Record retention and data destruction polices help ensure that SLDS data are handled securely and in accordance with federal, state, and agency requirements. The policies must balance a number of considerations, including the SLDS program's legal and operational responsibilities as well as its technical capacity for managing and storing data. Good record retention and data destruction policies lay out comprehensive guidance for managing each different type of data contained in the SLDS throughout the data life cycle. By establishing strong policies and revising them to address emerging technical capabilities and challenges, SLDS programs can keep sensitive personal information secure while supporting research, state policies, and instructional decisions that rely on SLDS data.

Additional Resources

Privacy Technical Assistance Center (PTAC): Best Practices for Data Destruction
https://studentprivacy.ed.gov/resources/best-practices-data-destruction

PTAC: The Family Educational Rights and Privacy Act Guidance for Reasonable Methods and Written Agreements
https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements

SLDS Guide: Developing a Process for Managing Research Requests
https://slds.ed.gov/#communities/pdc/documents/15117

SLDS Guide: Developing Effective Data Policies and Processes
https://slds.ed.gov/#communities/pdc/documents/18418

SLDS Issue Brief: Preparing for an SLDS Audit
https://slds.ed.gov/#communities/pdc/documents/15092

SLDS Webinar: Considerations for Preparing for and Responding to a Federal Audit
https://slds.ed.gov/#communities/pdc/documents/18226

SLDS Webinar: State Approaches to Cloud Technology
https://slds.ed.gov/#communities/pdc/documents/19992