

Federal Laws Are Not a Barrier to Connecting Data within a Statewide Longitudinal Data System



People need easier access to information that helps them make education and employment decisions. Statewide longitudinal data systems (SLDSs) by design facilitate longitudinal data connections across the early childhood, K–12 education, postsecondary education, and workforce sectors. When building these connections, understanding how different federal requirements apply to different sectors can be difficult, and at times concerns about what is permissible can derail progress on connecting data in new ways to inform new questions.

States can tap their SLDSs to combine cross-agency data for ongoing purposes, instead of using ad hoc approaches to connect data across sectors to address specific use cases. Federal laws have been interpreted to permit the use of SLDSs to manage data from multiple agencies. The most robust and sustainable SLDSs are designed with frameworks in place to meet the requirements of federal laws that apply when combining data from multiple agencies. This resource discusses common myths about integrating data within an SLDS for ongoing uses.

MYTH

Data can be integrated within an SLDS only if done in the context of a specific research or evaluation project.

FACT

The US Department of Education (ED) interprets the Family Educational Rights and Privacy Act (FERPA) to enable the integration of K–12 education records into an SLDS to facilitate all permitted data uses, even if a specific project is not contemplated at the time of integration.

- ➔ The Privacy Technical Assistance Center (PTAC) published guidance in 2017 applying FERPA to SLDSs (described in the guidance as state-level integrated data systems) that allows for data from multiple government agencies to be linked.¹
- ➔ The legal arrangements for disclosing education records to an SLDS are structured around the FERPA exception to consent for disclosures. Under FERPA, personal information can be disclosed to authorized representatives of state education authorities for the purposes of an audit or evaluation of federal or state-supported education programs.
- ➔ SLDSs often engage an entity that is separate from contributing agencies, such as an independent government office or a university, to host and operate the system. This entity can manage the work required to ensure that there is ongoing capacity for approved data uses involving integrated data.

- State education agencies (SEAs) that contribute data to an SLDS need to comply with the FERPA requirements, including a written agreement with the entity administering the SLDS that designates the entity as the agency's authorized representative, specifies the data to be disclosed, and uses reasonable methods to ensure proper use and protections of the data.
- The agency must consider whether the entity managing the SLDS will be the only entity authorized to use the integrated data within the SLDS or whether data may be redisclosed to other organizations.
- If the entity managing the SLDS is authorized to redisclose integrated data from the SLDS to third parties, the written agreement between the agencies and the managing entity must include that authorization and describe all of the requirements applicable to the redisclosure.

FACT

Nothing in federal law prevents including early childhood, college (regardless of funding), or workforce training data in an SLDS.

- **Early childhood:** FERPA applies to all education institutions that receive federal funding from ED for any education program.² Education programs encompass all types of early childhood education programs, including Head Start, Early Head Start, child care, state prekindergarten, and early intervention services for infants and toddlers and their families.³ Under the FERPA exception to consent for disclosures, these programs can disclose personal information to authorized representatives of state education authorities for the purposes of an audit or evaluation of federal or state-supported education programs.⁴
- **Colleges:** FERPA applies to any private colleges that participate in federal financial aid programs, including work-study. As a result, almost all private colleges are covered by FERPA. Further, nothing in federal law prevents a private college not covered by FERPA from contributing data to an SLDS.
- **Workforce training:** The Workforce Innovation and Opportunity Act (WIOA) requires states, local areas, and eligible training providers to report on indicators of performance that include employment outcomes and requires states to conduct ongoing evaluations of the WIOA core programs. WIOA does not restrict the use of an SLDS for these purposes. WIOA requires states to comply with FERPA when carrying out WIOA's requirements. FERPA's audit or evaluation of state or federal programs exception applies to such disclosures. FERPA's definition of education programs includes job training, career and technical education, and adult education.⁵

MYTH

An SLDS cannot include financial aid information or link it to data from other sectors.

FACT

An SLDS can include financial aid data if the data is used to support the ongoing administration of student aid programs, including the evaluation or audit of such programs.

- Under the Higher Education Act and its regulations, state agencies that administer state student aid programs can receive certain data from ED concerning Free Application for Federal Student Aid (FAFSA) applicants through a Student Aid Information Gateway (SAIG) Participation Agreement.⁶ ED provides a state agency with the Institutional Student Information Record (ISIR) for students within their state, which includes the information from the student's FAFSA submission to ED.
- Under the SAIG agreement, ISIR data can be used only to (a) calculate student financial aid awards, (b) conduct research necessary for the proper administration of a state student aid program, and (c) verify data provided by an applicant on state student aid applications.
- Only authorized personnel in a state agency can access ISIR data. Authorized personnel include employees of the agency, contractors, and other parties who are under the direct control of or bound to the agency.

- ➔ A state agency can provide ISIR data to an entity administering an SLDS through a written agreement to both protect the data and ensure its proper use, including confirming that any research or evaluation project supports student aid programs and complies with terms of the SAIG agreement.

MYTH

Centralizing data from multiple agencies within an SLDS inherently creates more risk than maintaining the data separately.

FACT

Centralizing data within an SLDS can strengthen the privacy and security of the data.

- ➔ When states centralize data in an SLDS, they can apply data privacy and security approaches at scale. Otherwise, each agency or entity managing data collections may implement separate protocols, which is a less secure approach and not cost effective.
- ➔ SLDSs can mask or remove personally identifiable information from already linked data *before* the data is used for any research or evaluation purposes. This approach involves much less risk than systems that require separate data from separate agencies to be submitted to a researcher with all personally identifiable variables still attached for linking purposes.
- ➔ “Cloud-based” systems can provide the data needed for a project within a secure space within the cloud, without the data ever leaving the multiple layers of security the state has established for access to data from the SLDS. The cloud-based project space also enables continuous monitoring of access to and use of the environment.

MYTH

Other federal laws, such as the Children’s Online Privacy Protection Rule (COPPA), the Protection of Pupil Rights Amendment (PPRA), and the Health Insurance Portability and Accountability Act (HIPAA), are more restrictive than FERPA and limit the integration of data within an SLDS.

FACT

While laws such as COPPA, PPRA, and HIPAA have specific requirements for the collection and use of personal information, they do not prevent the integration of data within an SLDS.

- ➔ COPPA does not apply to schools or education agencies that collect personal information for educational purposes and therefore would not limit the ability of data initially collected by schools to be submitted to an SEA and integrated into an SLDS.
- ➔ PPRA does not address the use of data a school or district may submit to an SEA or that the agency may integrate into an SLDS.
- ➔ HIPAA does not apply to school or education agencies that collect health information that is incorporated into students’ education records, and it does not limit the ability of a state agency to incorporate such data into an SLDS with appropriate compliance and security steps expected by HIPAA.

ADDITIONAL RESOURCE

Getting the Facts Straight about Statewide Longitudinal Data Systems: States are in different stages of updating their SLDSs to meet these data access needs. As state leaders do this important work, they must be attentive to more than just technical upgrades. They must also navigate issues including a complicated landscape of legal frameworks, data sharing agreements, and data privacy and security requirements. This resource discusses common education and workforce data privacy questions and their implications for connecting data across specific sectors. Download it at dataqualitycampaign.org/slids-facts.

Endnotes

- 1 Privacy Technical Assistance Center, Integrated Data Systems and Student Privacy (US Department of Education, January 2017), https://studentprivacy.ed.gov/sites/default/files/resource_document/file/IDS-Final_0.pdf. The information in this section is generally drawn from the PTAC guidance and supplemented by the authors' and the Data Quality Campaign's direct experience with integrated data systems.
- 2 34 CFR § 99.1(a).
- 3 34 CFR § 99.3.
- 4 34 CFR § 99.31(a)(3) and 99.35.
- 5 34 CFR § 99.1(a).
- 6 The current form of the SAIG agreement is available at <https://fsawebenroll.ed.gov/PMEnroll/public/AgencyAgreement.pdf>.