

Getting the Facts Straight about Statewide Longitudinal Data Systems



People need easier access to information that helps them make education and employment decisions. States are in different stages of updating their statewide longitudinal data systems (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 also must navigate issues including a complicated landscape of legal frameworks, data sharing agreements, and data privacy and security requirements. A comprehensive approach to addressing these frameworks and requirements does not need to be a barrier to designing an SLDS; in fact, it sets a strong foundation for better cross-agency collaboration in service of providing better information to people.

Existing Federal Laws Permit Cross-Sector Data Linkages

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. If states are attentive to how these requirements must be applied to each sector, current laws will not prohibit these connections. This section discusses common education and workforce data privacy questions and their implications for connecting data across specific sectors.

Connecting early childhood and K–12 education data

Building connections between early childhood data and K–12 data enables insights about children’s experiences in early life that can help those supporting them to understand students’ readiness for kindergarten, address their nonacademic needs, and provide information back to early childhood program providers. Because of the dispersed nature of early childhood programs, states seeking to connect early childhood and K–12 data within an SLDS often have to navigate perceptions about what laws apply and how those laws must be implemented. Early childhood and K–12 education data *can* be connected, including in the specific instances discussed in this section.

MYTH

Because the Family Educational Rights and Privacy Act (FERPA) does not apply to early childhood providers, an SLDS cannot include their data.

FACT

Nothing in federal law prevents including early childhood program data in an SLDS.

- ➔ FERPA applies to all education institutions that receive federal funding from the US Department of Education (ED) for any education program.¹ 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.²
- ➔ Under FERPA, early childhood education 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.³

HEAD START PRIVACY PROVISIONS

Head Start program regulations include privacy provisions that generally mirror FERPA.

- ➔ They enable officials of the Head Start program to disclose child records without consent to a federal or state entity:
 - In connection with an audit or evaluation of education or child development programs; or
 - For enforcement of or compliance with federal legal requirements of the program.
- ➔ Head Start programs must have a written agreement with the state entity and maintain oversight with respect to the continued use of the records. Some states have addressed the oversight expectation through including Head Start representatives on SLDS governance bodies.

MYTH

The Health Insurance Portability and Accountability Act (HIPAA) prevents early childhood service providers from connecting health, human services, and education records.

FACT

HIPAA allows early childhood service providers to connect health, human services, and education records as long as the linkage and use of health records complies with FERPA and any applicable state privacy protections.

- ➔ HIPAA applies only to protected “health information,” which is defined in the HIPAA regulations as information that “relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.”⁴
- ➔ Early childhood data is covered by FERPA or Head Start privacy regulations, and the HIPAA Privacy Rule excludes any health information that is in education records covered by FERPA from the definition of “protected health information” that is subject to HIPAA requirements.⁵

MYTH

FERPA prevents states from giving early childhood education providers data about their former students once those students are in elementary school.

FACT

FERPA authorizes early childhood education providers to access their former students’ information.

- ➔ A state can provide a child’s personally identifiable information (PII) to an authorized representative for evaluations of federal or state-supported education programs, including early childhood education programs.⁶
- ➔ A state education agency (SEA) can establish agreements with providers that (a) formally designate each provider as an authorized representative and (b) obtain the provider’s agreement to use the information only for program evaluation and protect it from further disclosures or other uses.

The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that governs the privacy and security of personal health information. The law sets out specific requirements for the use and disclosure of health information by covered entities.



Connecting K–12 and postsecondary education data

Using SLDSs to build connections between K–12 and postsecondary data can smooth students' transitions between high school and college by providing information that helps students make decisions about postsecondary programs, helps institutions understand the readiness of enrolling students, and removes barriers to enrollment through auto-admission programs. FERPA and other laws allow for data connections that support these and other critical uses.

MYTH

FERPA prevents SEAs from sharing K–12 information with postsecondary institutions.

FACT

FERPA authorizes SEAs to share K–12 information with postsecondary institutions.

- ➔ SEAs receive data from schools or school districts through FERPA's exception to consent for audit, evaluation, enforcement, or compliance purposes.⁷
- ➔ An SEA may redisclose the data under any of the exceptions to consent listed in FERPA, including sharing data with officials of another school or postsecondary institution where the student seeks to enroll or in connection with financial aid applications and receipt.
- ➔ An SEA can determine which disclosures to make on behalf of the schools and districts it oversees.

MYTH

FERPA prevents states from providing high school leaders and educators with relevant postsecondary information about their former students (e.g., high school feedback reports).

FACT

FERPA allows high school leaders and educators to access data on college enrollment, outcomes, and other types of information.

- ➔ A state can provide student PII to an authorized representative in connection with an evaluation of federal or state-supported education programs, which include all of the instructional and counseling programs of a public high school and could include programs for nonpublic schools.⁸
- ➔ An SEA can establish agreements that (a) formally designate each school (or district, on behalf of a school or schools) as an authorized representative and (b) obtain the school's or district's agreement to use the information only for program evaluation and protect it from further disclosures or other uses.

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.⁹ 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

FERPA does not apply to private colleges, and their data cannot be linked within an SLDS.

FACT

Neither FERPA nor any other federal law prevents including data in an SLDS from any college provider, regardless of the funding the provider receives.

- ➔ 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.

Connecting education and employment data

Many people navigate between education and employment opportunities. Individuals need to understand how different types of education or training programs align with career goals, and leaders need to understand if the skills of people in the state align with future needs of the economy. Robust linkages between education and workforce data are allowable and can answer these types of questions, but building these linkages requires a solid framework for navigating multiple laws. The following section describes some common questions about how education and workforce laws apply when linking data across these sectors.

MYTH

Data from workforce training providers cannot be linked within an SLDS.

FACT

Federal law poses no barrier to including data in an SLDS from workforce training providers.

- ➔ 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.
- ➔ Workforce training programs that do not receive federal funding from ED may be approved as eligible training providers under WIOA and thus subject to reporting expectations under WIOA.
- ➔ 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.¹⁰

MYTH

FERPA and federal unemployment insurance regulations restrict the sharing of employment outcomes data with education and training providers.

FACT

Neither FERPA nor federal unemployment insurance regulations restrict the sharing of employment outcomes data with education and training providers.

- ➔ Employment outcomes records are not subject to FERPA, as they are not directly related to a student and are not maintained by an education agency or institution.¹¹
- ➔ A state agency administering unemployment compensation (UC) laws must comply with the Department of Labor (DOL) confidentiality and disclosure regulations governing these records when the agency shares employment outcomes records.¹²
- ➔ A state agency administering UC information (or its designee) can provide confidential UC information to *public* universities for approved data use purposes through an agreement with the postsecondary institution to meet DOL's regulatory requirements.¹³
- ➔ A state agency administering UC information (or its designee) can provide employment outcomes data to *private* education and training providers by:
 - Sharing aggregate reports that do not include confidential information; or
 - Establishing a system for designating the private education and training provider as an agent of a public official for approved data use purposes.¹⁴

MYTH

State agencies administering UC programs are restricted from sharing data with an SLDS or can do so only if they perform all data matching.

FACT

State agencies administering UC programs can share data through an SLDS and are not required to perform all data matching to support these purposes.

- According to DOL's regulations,¹⁵ state UC agencies may disclose confidential UC information, including wage records, to "public officials" in the performance of their official duties¹⁶—which includes applicable research, program performance accountability requirements, and reporting.¹⁷
- The state UC agency may disclose confidential UC information to the entity that administers the SLDS, provided the use meets the definition of official duties (as described in the previous bullet).
- The SLDS administrator must maintain the confidentiality of any UC information that alone or in combination with other available information would reveal identifying information about any individual or any past or present employer or employing unit.¹⁸

Federal Laws Are Not a Barrier to Integrating Data within an SLDS

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 section 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

ED interprets FERPA to enable an SEA to integrate 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.¹⁹
- The legal arrangements for disclosing education records to an SLDS are structured around the FERPA exception to consent for disclosures to an authorized representative of state and local education authorities for an audit or evaluation of federal or state 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.
- 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.

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 PII 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 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.

The Children’s Online Privacy Protection Rule (COPPA) is a federal law that governs the online collection of personal information for individuals under the age of 13. The law requires operators of commercial websites and online services to obtain verifiable personal consent from children before collecting personal information from children.

The Protection of Pupil Rights Amendment (PPRA) requires that schools obtain parents’ consent before requiring children to participate in any survey, analysis, or evaluation funded by ED that involves certain topics, such as politics, religious beliefs, or mental health. PPRA also requires parental notice and opt-out opportunities for the collection of information from students for most marketing purposes.

Definitions

Following are key terms used in this brief and how they are defined in FERPA:

Audit or Evaluation Exception: The FERPA provision that permits the disclosure of personal information without consent to authorized representatives of state and local education authorities in connection with an audit or evaluation of federal or state-supported education programs or for the enforcement of or compliance with federal legal requirements that relate to those programs.²⁰

Authorized Representative: Any entity or individual designated by a state or local education authority to conduct—with respect to federal or state-supported education programs—any audit or evaluation or any compliance or enforcement activity in connection with federal legal requirements that relate to those programs.²¹ Disclosures to an authorized representative require written agreement and the use of reasonable methods to ensure to the greatest extent practicable FERPA compliance by the authorized representative.

Education Program (subject to FERPA): Any program principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education.²² To be subject to FERPA, an education program must be provided by an education agency or institution receiving funds from ED.²³

Evaluation: All types of studies, assessments, measurements, appraisals, research, and other efforts, including analyses of statistical or numerical data derived from education records.²⁴

Feedback Information: Information from one segment of the education continuum to an education program in an earlier segment of the continuum, such as information on elementary outcomes provided to early childhood education administrators and programs or information on postsecondary outcomes provided to high school administrators and programs.

Integrated Data System: A data system that allows linkage of administrative data from multiple government agencies within a common environment for further analysis and utilization.

State Education Agency (SEA)/State Education Authority: The state board of education or other agency or officer primarily responsible for the state supervision of public elementary schools and secondary schools or, if there is no such officer or agency, an officer or agency

designated by the governor or by state law. An SEA is not considered an “education agency” or “institution” under FERPA. Instead, FERPA imposes obligations on SEAs as “state educational authorities.” The FERPA regulations do not define “state and local educational authorities,” but ED has interpreted the term to include (1) SEAs; (2) school districts; (3) state postsecondary commissions; (4) the Bureau of Indian Education; and (5) other entities that are responsible for and authorized under local, state, or federal law to supervise, plan, coordinate, advise, audit, or evaluate elementary, secondary, or postsecondary federal or state-supported education programs and services in a state.

Statewide Longitudinal Data System (SLDS): A statewide data system that connects individual-level data from participating state agencies over time. At a minimum, SLDSs connect data from early childhood education, K–12 education, postsecondary education, and the workforce.

Unemployment Compensation (UC) Information: Information in the records of a state agency charged with the administration of UC laws that pertains to the administration of those laws, including information about the wages paid to an individual, Social Security account numbers, and the employer paying wages.²⁵ (Federal regulations use the term “unemployment compensation,” not “unemployment insurance.”)

Public Official (in relation to UC information): An official, agency, or public entity within the executive branch of federal, state, or local government that has responsibility for administering or enforcing a law.²⁶ This category also includes public postsecondary education institutions, publicly governed and publicly funded community and technical colleges, performance accountability and customer information agencies, the head of local workforce areas under WIOA, state education authorities under FERPA,²⁷ and agents or contractors of public officials.²⁸

Official Duties (in relation to UC information): Administration or enforcement of law or the execution of the official responsibilities of a public official, including research related to administering a law, state and local performance accountability under WIOA, and as otherwise required for education or workforce training program performance accountability and reporting under federal or state law.²⁹

Endnotes

- 1 34 CFR § 99.1(a).
- 2 34 CFR § 99.3.
- 3 34 CFR § 99.31(a)(3) and 99.35.
- 4 45 CFR § 160.103.
- 5 *Ibid.*
- 6 34 CFR § 99.31(a)(3) and 99.35.
- 7 *Ibid.*
- 8 *Ibid.*
- 9 The current form of the SAIG agreement is available at <https://fsaweбенroll.ed.gov/PMEnroll/public/AgencyAgreement.pdf>.
- 10 34 CFR § 99.1(a).
- 11 34 CFR § 99.3.
- 12 20 CFR Part 603. Part 603 distinguishes between required and permissive disclosures. The provision of UC wage records to an SLDS would constitute a permissive disclosure.
- 13 20 CFR § 603.10.
- 14 20 CFR § 603.5(f).
- 15 20 CFR Part 603. Part 603 distinguishes between required and permissive disclosures. The provision of UC wage records to an SLDS would constitute a permissive disclosure.
- 16 20 CFR § 603.5.
- 17 20 CFR § 603.5(e).
- 18 20 CFR § 603.4(b).
- 19 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.
- 20 34 CFR § 99.31 and 99.35.
- 21 34 CFR § 99.3.
- 22 *Ibid.*
- 23 34 CFR § 99.1.
- 24 73 Fed. Reg. 15586.
- 25 20 CFR § 603.2.
- 26 20 CFR § 603.2(d)(1).
- 27 *Ibid.*
- 28 20 CFR § 603.5(f).
- 29 20 CFR § 603.5(e).