Integrated Data Systems and Student Privacy

About PTAC

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems. More PTAC information is available at https://studentprivacy.ed.gov.

PTAC welcomes input on this document and suggestions for future technical assistance resources relating to student privacy. Comments and suggestions can be sent to PrivacyTA@ed.gov.

Introduction

In the context of this document, "**educational authorities**" will refer to both state educational authorities (e.g., state educational agencies and higher education governing boards) and local educational authorities (e.g., school districts), unless otherwise differentiated.

Educational authorities and policymakers are increasingly focused on protecting student privacy while using data to inform program and policy decisions. Data from more than one government agency is often analyzed to more holistically inform these decisions. This has led to the development of integrated data systems (IDSs) that allow linkage of administrative data from multiple government agencies. IDSs can be used for multiple purposes; this document discusses how educational authorities can use an IDS for program evaluation and research, consistent with the Family Educational Rights and Privacy Act (FERPA)[1] and privacy best practices. In some cases, an educational authority hosts the IDS (e.g., statewide longitudinal data system). The primary focus of this guidance, however, is on those cases in which an educational authority does not host the IDS.

The diversity of IDS structures, governance models, and intended uses presents complex legal and policy issues relating to privacy. Educational authorities that seek to participate in an IDS face questions as to how they can protect student privacy in compliance with FERPA and other applicable privacy laws while disclosing, without the prior written consent of parents (or of eligible students[2]), personally identifiable information (PII) from education records to an IDS Lead (as defined below). This guidance document provides background information on what an IDS is and why educational authorities may choose to participate in one, and clarifies how such authorities can participate in an IDS while ensuring student privacy in compliance with FERPA.

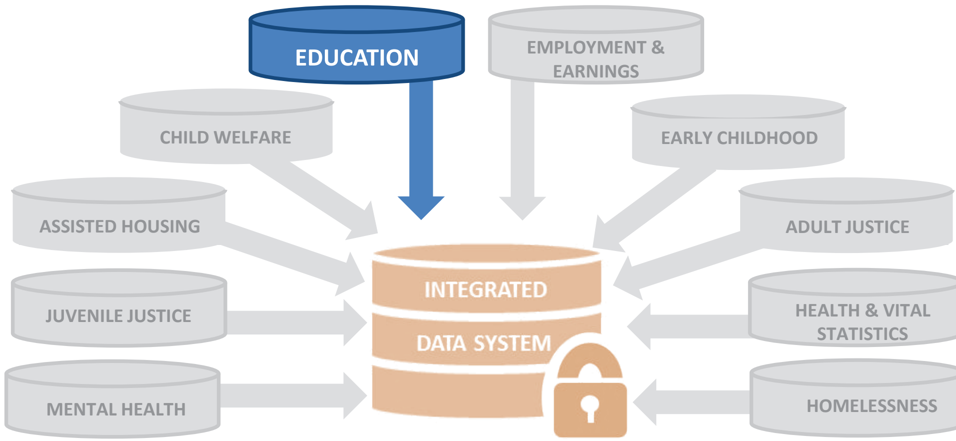
Please note, because of the diversity of IDS structures, the fact that state laws may impose more stringent privacy protections than those of FERPA, and the fact that other federal and state privacy laws may also apply, educational authorities should consult with counsel *before* participating in an IDS.

---

[1] See 20 U.S.C. § 1232g and 34 CFR Part 99.
[2] "Eligible students" are those who are 18 years of age or older or attending an institution of postsecondary education. See 34 CFR § 99.3.

Table of Contents

What Is an Integrated Data System?



An IDS allows linkage of administrative data from various government agencies for more holistic information to

- better understand the complex needs in communities;
- inform the design of new strategies and interventions to address those needs; and
- evaluate the effectiveness of programs and policies on the desired outcomes.

Entities that host and operate IDSs (IDS Leads) include, but are not limited to, state or local government agencies, universities, nonprofit organizations, and in some cases, contractors of the aforementioned entities. Agencies that participate in IDSs include, but are not limited to, those responsible for public education, public benefits, child welfare services, employment and training, criminal justice, mental health services, physical health services, public housing, and homeless shelter systems.

The participating agencies generally provide the IDS Lead an extract or access to their data on a regular basis (e.g., daily, weekly, monthly, or annually), including certain PII from education records (e.g., name and date of birth) needed to match individual records across systems. Often, IDSs use a data warehouse model that links and stores data from all partners in a centralized data system so that individual requests for access can be evaluated. The integration of data from multiple government agencies means that multiple federal and state privacy and confidentiality laws and their corresponding access and use restrictions often apply. Successful implementation of an IDS, therefore, requires a strong governance model to manage the security of the data and to limit access to authorized individuals working on approved projects. Federal requirements and best practice recommendations for IDSs that involve the non-consensual disclosure of education data are discussed below.

Some IDSs integrate data using a federated model, rather than the data warehouse model discussed above. In a federated model, the participating agencies maintain control of the data in their source systems. Data are only accessed and integrated to fulfill a specific, approved request. If the method to integrate data does not store any linked data with PII from education records, then only the specific requests seeking PII from education records in the source systems of educational authorities would need to be reviewed for FERPA compliance. For a federated model, the *Approving the Use of Integrated Data* and *Best Practices* sections of this guidance are most applicable.

While this guidance focuses on the legal framework to protect student privacy and use integrated data for research and evaluation, some IDSs are set up to allow staff at participating agencies to access individual-level integrated data to provide services to the clients/students whom they serve. These types of systems should be set up to only allow access to individual records in limited cases where an individual has a need to see those records for authorized program purposes and provided such access is permissible through either complying with the consent provisions or with an exception to the consent provisions as set forth in applicable federal and state privacy laws. For example, a child welfare caseworker may be able to access PII from a student's education records through an IDS if he or she obtains prior written consent from the student's parent or if a federal or state law permits access in the absence of such consent, such as pursuant to the Uninterrupted Scholars Act.[3]

Why Are Educational Authorities Participating?

As this document will discuss, the decision by educational authorities to create an IDS, or to participate in an IDS in their communities, necessitates a vigilance toward protecting student privacy and ensuring compliance with applicable federal and state privacy laws, as well as substantial and ongoing investment in data governance and oversight. That said, many communities across the country have determined that these investments may be advantageous for evaluating the efficacy of their education programs and for improving student outcomes.

The integration of education data with administrative records from other government agencies enables state and local education officials, policymakers, and researchers to examine trends and patterns in student performance and outcomes that are impossible to assess by examining education data on its own. Some of the myriad types of analyses that may be informed by the use of integrated data include (1) better understanding the complex needs of students within the broader context of their communities; (2) informing the design of new strategies and interventions to address those needs; and, (3) evaluating the effectiveness of policies and programs on achieving their intended outcomes.

Educational authorities may also choose to use an IDS to help meet their own internal data and analytic needs. In a period of declining and constrained resources for public education,[4] many educational authorities lack the internal expertise and capacity to manage and analyze the data needed for effective data-informed decisionmaking. Participating in an IDS may therefore afford those educational authorities access to an integrated data infrastructure and analytic expertise.

As with all data decisions, educational authorities should carefully weigh the potential benefits of participating in an IDS against all the associated costs before deciding if partnering with an IDS is a worthwhile investment. Additionally, participation should be evaluated based on a number of privacy, security, and data governance best practices.

[3] The Uninterrupted Scholars Act, Pub. L. No. 112-278, amended FERPA to, among other things, permit the non-consensual disclosure of student education records to child welfare agency caseworkers or other representatives of a state or local child welfare agency or tribal organization who have the right to access a student's case plan, as defined and determined by the state or tribal organization, when such agency or organization is "legally responsible, in accordance with State or tribal law, for the care and protection of the student." 20 U.S.C. § 1232g(b)(1)(L).

[4] https://nces.ed.gov/fastfacts/display.asp?id=66

FERPA Compliance

FERPA is a federal law that protects the privacy of student education records and gives parents and eligible students certain rights with respect to education records, including under certain circumstances rights of inspection and review[5] and generally, the right to consent to the disclosure of these records.[6]

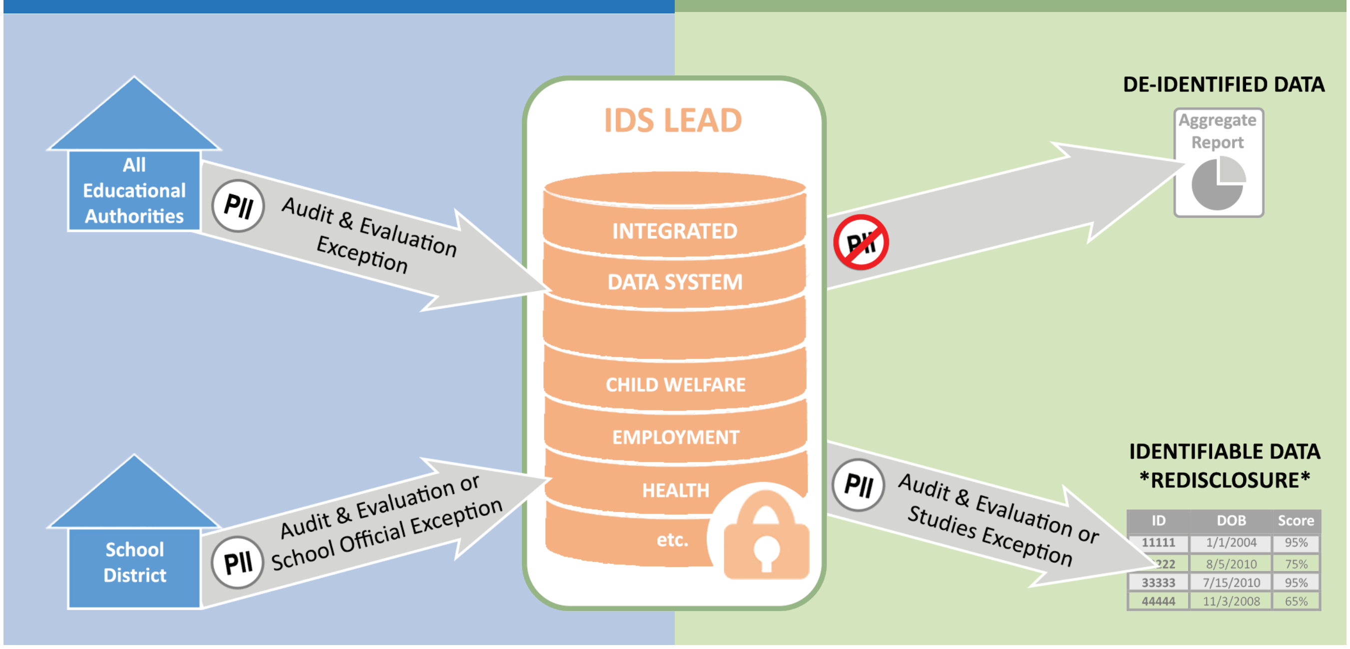
Under FERPA, a parent or eligible student must provide a signed and dated written consent before an educational agency or institution discloses PII from a student's education records, unless the disclosure meets one of the permissible exceptions to FERPA's written consent requirement.[7] PII refers to information, such as a student's name or identification number, that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.[8] FERPA applies directly to all educational agencies and institutions that receive funds under any program administered by the Secretary of Education (Department).[9] Private schools at the elementary and secondary levels generally do not receive funds from the Department and are, therefore, not subject to FERPA.

[5] See 34 CFR Part 99, Subpart B.
[6] See 34 CFR § 99.30.
[7] See 20 U.S.C. §§ 1232g(b)(1), (b)(2), (b)(3), (b)(5), (b)(6), and (b)(7), (h), (i), and (j); 34 CFR §§ 99.30(a) and 99.31.
[8] See 34 CFR § 99.3.
[9] See 34 CFR § 99.1(a).

FERPA Compliance Overview

It is important to understand that from a data-sharing perspective, there are two stages of IDS participation. The FERPA compliance issues and best practices are different for each stage. The following illustration includes high-level descriptions of each stage. More in-depth explanations and examples will follow. A one-page summary of the legal framework can be found on page 23.

STAGE 1	STAGE 2
Becoming an IDS Partner: Establishing a Data Governance Framework and Integrating Education Data into the IDS	**Approving the Use of Integrated Data: Reviewing Research Requests for FERPA Compliance and Releasing the Results of those Analyses**
Unless an educational authority intends to operate the IDS, participation in an IDS requires disclosure of PII from students' education records to the third party that will be hosting and operating the IDS (IDS Lead). To be permissible under FERPA, this disclosure must be made with the written consent of the parent or eligible student or it must satisfy one of FERPA's exceptions to the requirement for written consent. All educational authorities may explore the audit and evaluation exception to consent to participate. If the educational authority is a school district, it may also explore the school official exception to consent to participate.	*Once education data are integrated with the IDS, each prospective use of any integrated data containing PII from education records should be reviewed, within the context of the IDS data governance framework, for compliance with FERPA and other applicable federal and state confidentiality and privacy provisions and adherence to established best practices. A key distinction in approving the release of the results of analyses using integrated data is whether they will be released in a de-identified or identifiable format.*



Becoming an IDS Partner: Establishing a Data Governance Framework, and Integrating Education Data into the IDS (Stage 1)

The first step in working with an IDS Lead is to create an integrated data infrastructure. This generally involves a commitment from the educational authority to provide administrative data, in the form of student education records, to the IDS Lead on a regular and recurring basis. The IDS Lead then links these education records to data received from other participating agencies, creating the ongoing capacity to access integrated data for more comprehensive research and evaluation. The decision to join an IDS, therefore, should not be based on a one-time need for integrated data, but rather on an ongoing desire to use integrated data to answer key questions for better data-informed decisionmaking.

In order to match PII from students' education records with individual-level records from other government agencies, the IDS Lead needs access to PII from student education records, which often includes information such as name and date of birth. The educational authority may not disclose such PII, however, unless the parent or eligible student has provided a signed and dated written consent, or unless the disclosure meets one of FERPA's exceptions to consent.[10]

There are two exceptions to FERPA's general requirement of consent that may allow an educational authority to disclose PII from education records to an IDS Lead without consent. All educational authorities may explore the audit and evaluation exception to consent to make the disclosures of PII from students' education records to the IDS Lead. If the educational authority is a school district, it may also explore the school official exception to consent to make the disclosures of PII from students' education records to the IDS Lead. The criteria under each exception are described below.

Please note that while this document focuses on the requirements and applicability of FERPA to operating and participating in an IDS, it is important to recognize that other state and federal laws may provide additional protections regarding the use and disclosure of PII or other data in the IDS. Accordingly, stakeholders should contact their legal counsel for guidance on the applicability of these laws to the circumstances surrounding their IDS operation or participation. One such law is the Individuals with Disabilities Education Act (IDEA), which applies to the records of children referred to programs that provide IDEA services to children with disabilities. If a student whose PII is subject to FERPA also is referred to, eligible for, or receives services under, either Part C or Part B of the IDEA, any disclosures of PII regarding that student must comply with the applicable confidentiality regulations in Part C or Part B of the IDEA in addition to the requirements identified in this document. An overview of IDEA in the context of IDS can be found on page 15.

Additionally, educational authorities should evaluate participation based on a number of privacy, security, and data governance best practices, including a thorough review of the IDS Lead's security and governance plans and compliance track record, staff qualifications, previous research and analysis products, and feedback from existing agencies using the IDS.

Participating in an IDS Using the Audit and Evaluation Exception

FERPA's audit and evaluation exception to consent[11] can be explored by both state educational authorities (e.g., state educational agencies and Higher Education Governing Boards) and local educational authorities (e.g., school districts) for the first stage in IDS participation. We have generally

---

[10] See 20 U.S.C. §§ 1232g(b)(1), (b)(2), (b)(3), (b)(5), (b)(6), and (b)(7), (h), (i), and (j); 34 CFR § 99.31.
[11] See 20 U.S.C. §§ 1232g(b)(1)(C), (b)(3), and (b)(5); 34 CFR § 99.31(a)(3) and 99.35.

interpreted the term "state and local educational authority" to refer to an entity that is 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 the state. Therefore, the state or local educational authority may access the PII from education records without consent in connection with an audit or evaluation of a federal- or state-supported education program. The FERPA regulations define "Education program"[12] to mean:

> *any program that is 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, and any program that is administered by an educational agency or institution.*[13]

These state and local educational authorities are permitted to partner with an IDS Lead (without written consent of the parent or eligible student) through the audit and evaluation exception.[14] The specific purpose for which PII from education records is disclosed to the IDS Lead under this exception is to facilitate future evaluations of federal- or state-supported education programs by establishing linked data. For example, if a state educational authority partners with an IDS that has labor and wage data, then it is building capacity to regularly evaluate federal- and state-supported education programs for which employment and wage outcomes are relevant.

The audit and evaluation exception would generally permit disclosures of PII from education records to an IDS Lead if all of the following criteria are met:

- ☑ **The state or local educational authority designates the IDS Lead as its "authorized representative"** for the purpose of auditing or evaluating a federal- or state-supported "education program" on its behalf.

- ☑ **The state or local educational authority enters into a written agreement with the IDS Lead** and the agreement, at a minimum:

    - designates the IDS Lead as the state or local educational authority's authorized representative;

    - specifies the PII from education records to be disclosed;

    - specifies that the purpose for which the PII from education records is disclosed to the IDS Lead is to carry out an audit or evaluation of a federal- or state-supported education program that the state or local educational authority has the federal, state, or local authority to carry out;

---

[12] See 34 CFR § 99.3.

[13] Students are not enrolled or participating in programs directly with the state educational authority, but the state educational authority must hold PII from education records due to its role in auditing and evaluating district- and school-level education programs.

[14] State and local educational authority officials who receive education records under an audit and evaluation exception are permitted to redisclose the records, without consent, to specific entities for other qualifying! purposes under 34 CFR § 99.31 including to authorized representatives of state and local educational authorities for the purpose of a qualifying audit, evaluation, or compliance and enforcement purpose, as noted in the regulation preamble, and provided the recordkeeping requirements in 34 CFR § 99.32 have been met. http://www2.ed.gov/policy/gen/guid/fpco/pdf/ht12-17-08-att.pdf

- specifies whether the IDS Lead is authorized to redisclose the PII from education records to a third party and, if so, the circumstances under which such redisclosure is permissible and the recordation requirements applicable to such redisclosure. It may be permissible for the IDS Lead to redisclose PII to a third party if the state or local educational authority has separately designated the third party as its authorized representative for purposes of auditing and evaluating federal- or state-supported education programs and the IDS Lead is named as the party to redisclose the data. Additionally, it may be permissible if the third party is a subcontractor of the IDS Lead to support the audit and evaluation that the IDS Lead was authorized to perform, provided the same written agreement requirements are applicable to the subcontractor;

- includes a description of the activity with sufficient specificity to make clear that the work falls within FERPA's audit and evaluation exception, including a description of how the PII will be used;

- requires the IDS Lead to destroy PII from education records when the information is no longer needed for the specified purpose;

- specifies the time period in which the PII will be destroyed; and

- establishes policies and procedures consistent with FERPA and other federal and state confidentiality and privacy provisions to protect PII from unauthorized use and disclosure.

☑ **The state or local educational authority uses reasonable methods to ensure to the greatest extent practicable that the IDS Lead uses, protects, and destroys the PII from education records in compliance with FERPA's requirements.**[15]

☑ **The state or local educational authority must ensure that a record of each request for access to and each disclosure of PII from the education records of each student is maintained, which includes the names of any additional parties to whom the PII is disclosed and their legitimate interests, unless the record is maintained instead by the educational agency or institution from which the PII originated.** FERPA's recordation requirements[16] must be met in order for an IDS Lead to further disclose PII from education records to other stakeholders.

Participating in an IDS Using the School Official Exception

If a school district is interested in participating in an IDS, the school official exception to consent[17] may be appropriate for the first stage of using an IDS. Under the school official exception, school districts may non-consensually disclose PII from student education records to an outside entity if the school district determines that said entity meets its criteria for being a school official (as defined in the school district's annual notification of FERPA rights), and has a "legitimate educational interest" in the PII (as defined in the school district's annual notification of FERPA rights). The outside entity must perform an institutional service or function for which the school district would otherwise use its own employees. In

[15] These requirements are discussed in PTAC's Guidance for Reasonable Methods and Written Agreements, available at https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements.

[16] See 34 CFR § 99.32(b)(2).

[17] See 20 U.S.C. § 1232g(b)(1)(A); 34 CFR 99.31(a)(1).

the case of an IDS, for example, the IDS Lead may perform, for the school district, the function of linking and storing education data, including maintaining security and controlling access to the data.

Another key requirement for the school official exception is that the IDS Lead must be under the direct control of the school district with regard to the use and maintenance of the disclosed PII from education records. While FERPA regulations do not specifically require a contract/written agreement for disclosures under the school official exception, if school districts wish to outsource services, a contract/written agreement signed by both parties and strong monitoring and oversight procedures to verify that the IDS Lead is complying with the agreed upon contract/written agreement terms, will help establish direct control. The contract/written agreement should contain all of the necessary legal provisions governing access, use, protection, and destruction of the PII.[18]

SCHOOL OFFICIAL COMPLIANCE CHECKLIST - the school official exception to consent would generally permit disclosures of PII from education records to an IDS Lead if <u>all</u> of the following criteria are met:

- ☑ **The entity seeking to participate in the IDS is a school district.** Only schools and school districts have the authority to designate a school official.

- ☑ **The IDS Lead performs an institutional service or function for which the school district would otherwise use employees.** In the case of an IDS, the IDS Lead may perform, for the district, the function of creating an integrated data infrastructure, including linking education data with other IDS data sources, maintaining security, and controlling access to the data.

- ☑ **The school district has determined that the IDS Lead has a "legitimate educational interest" and needs access to the PII to perform the required institutional service or function for the school district.** The definition of "legitimate educational interest" is at the discretion of the school district, but must be included in its annual notification of FERPA rights as stated below.

- ☑ **The school district's annual notification of FERPA rights includes criteria for who is designated as a school official and what constitutes a legitimate educational interest and the IDS Lead meets these criteria.** It is best practice to be transparent about disclosure and redisclosure policies to ensure parents and students fully understand who has access to the PII and how it is being used.

- ☑ **The IDS Lead is under the direct control of the school, with respect to the use and maintenance of the PII.**

- ☑ **The IDS Lead is subject to the same conditions governing the use and redisclosure of the PII that apply to other school officials under FERPA.** The parties that receive PII from education records under this exception may only use such PII for the purpose for which it was disclosed to them by the school district (i.e., to provide institutional services or functions to the school district). Further, FERPA requires that the school district use reasonable methods to

[18] Additional guidance on written agreements can be found in *The Family Educational Rights and Privacy Act Guidance for Reasonable Methods and Written Agreements*, available at https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements. (Note: this document discusses written agreements for the audit and evaluation and studies exceptions, but the criteria listed are relevant for compliance and best practices when using the school official exception as well).

ensure that school officials, including parties to whom institutional functions and services have been outsourced, obtain access to only those education records in which they have legitimate educational interests and are necessary to perform such institutional functions and services. Further disclosures of PII from education records by the IDS Lead to other stakeholders are only permissible under the direction of the school district, and in compliance with FERPA, and FERPA's recordation requirements must be met.

Establishing a Data Governance Framework

Prior to integrating any PII from education records into an IDS, educational authorities should ensure that the governance framework and documentation for the IDS meets all of the legal requirements for the relevant FERPA exception outlined above, ensures strong physical and IT security controls over the system, establishes sufficient oversight over the operation of the IDS, promotes transparency about the IDS's data practices, and establishes a framework for reviewing and approving individual uses of the integrated data. The Department has a number of recommendations for best practices regarding data security and transparency provisions to include, which are covered in the *Best Practices* section below.

Each IDS will reflect the unique needs and capabilities of its community and participants. Consequently, educational authorities seeking to participate in an IDS have a variety of options for structuring the data governance framework to be used. Some governance structures require extensive consideration and articulation of intended projects up front, pre-approving all permitted and intended projects and uses of the data in the IDS governance documents. At the other extreme, some IDS frameworks only establish broad evaluation goals up front, but defer consideration of all specific projects and evaluations until the IDS infrastructure has been established. Both approaches have advantages and disadvantages regarding the burden and oversight required for the creation of the IDS and during its subsequent operation, and the selection of which approach to take largely depends on the existing capacity and experience of the participating agencies and the IDS Lead. These options, and their implications for the operation of the IDS, are discussed further in the *Governance Models for Data Use* section below.

Approving the Use of Integrated Data: Reviewing Research and Evaluation Requests for FERPA Compliance and Releasing the Results of those Analyses (Stage 2)

The second stage of using an IDS is to manage access and use of the integrated data by the IDS Lead as well as other stakeholders, and to release the results of those uses back to the participating agencies and/or to the public.

Most IDS structures have the IDS Lead taking a primary role in summarizing, analyzing, and de-identifying data to make it useful to the various stakeholders who make requests. Some IDS frameworks also permit external organizations and research partners to submit requests to access and use identifiable integrated data. The range of permitted uses, the process for making requests, and the review and approval process for handling those requests should all be detailed in the data governance framework established during Stage 1. In Stage 2, the IDS Lead and the partner agencies should review these requests, and ensure that each use or release of data from the IDS is permissible under FERPA (and other applicable privacy laws). Evaluating whether a proposed use or release of data is permissible largely depends on whether the data are in identifiable form, who the requestor is, and what the requestor's purpose is for using the data.

Below are two common ways integrated data are shared with stakeholders:

1. **De-identified Data:** All direct and indirect identifiers have been removed, and there is no reasonable basis to believe that the remaining information can be used to identify an individual.

These de-identified data may be in the form of aggregate results or individual-level data. If the IDS Lead is releasing aggregate results, the IDS Lead should ensure it contains sufficient cell and subgroup sizes so that individual-level outcomes are not identifiable. If the request can only be fulfilled with individual-level data, then the IDS Lead should remove direct and indirect identifiers prior to release, along with other data that alone or in combination are linked or linkable to a specific student. One or more disclosure avoidance techniques may be required to ensure that the dataset is properly de-identified. When data are properly de-identified, there is no disclosure of PII from education records under FERPA, and no exception to consent is required. Additional information can be found in the *Using De-identified Data* section below.

2. **Identifiable Data**: In those limited instances in which PII from education records is required to meet the objectives of the project, then the IDS Lead may redisclose the PII if, and only if, it is approved by the educational authority and the redisclosure is permissible under a FERPA exception to the written consent requirement and complies with applicable FERPA recordation requirements and with any other applicable federal and state confidentiality and privacy provisions. The identifiable data may be in the form of aggregate/summary data or individual-level data. In all cases, the IDS Lead should only release the minimally required identifiers to meet the project objectives. These exceptions are described in the *Using Identifiable Data* section below.

It is important to be aware of the minimum amount and granularity of data needed to meet each request for integrated data. If a stakeholder's research or evaluation question can easily be answered with a summarized table or chart (de-identified), then that is the preferred method to minimize disclosures and risk. PII from education records may only be shared without consent when the disclosure falls under one of FERPA's exceptions to consent and complies with applicable FERPA recordation requirements and with any other applicable federal and state confidentiality and privacy provisions, and should only be shared if that granularity of data is needed to meet the stakeholder's project objectives. Please note that this guidance explores instances when disclosing PII from education records without consent is permissible. None of the data sharing discussed herein is required. Educational authorities should always review each request to evaluate its alignment with their priorities, potential to positively impact students and families, and the time and resources that would be needed to fulfill the request.

Regardless of whether the method to share data is identifiable or not, the IDS Lead may only access data for the uses permitted in the legal framework the educational authority established with the IDS Lead to become an IDS partner (Stage 1).

Audit & Evaluation Exception	School Official Exception
Staff of the IDS Lead may use the linked data internally to conduct analysis if it is a data analysis project (project) to audit or evaluate a federal- or state-supported education program. If the project aligns with an audit or evaluation described in the written agreement that created the integrated data infrastructure, then it may be conducted by staff of the IDS Lead under the existing agreement. If the project is not listed in the initial written agreement, but still aligns with an audit or evaluation of a federal- or state-supported education program, then the IDS Lead can enter into an additional written agreement with the educational authority to access linked data for the project.	Staff of the IDS Lead may use the linked data internally to conduct analysis if it is a project that the school district would otherwise conduct itself. To ensure that this is the case, the project request should come from the school district or be formally approved by the school district. The school district may approve requests either on a project-specific basis or by generating a list of pre-approved types of projects that may be conducted by staff of the IDS Lead.

In certain cases, an IDS can be very valuable operationally by using individual-level integrated data to improve services to children and families. This guidance document, however, focuses on the legal framework to use integrated data to inform and evaluate program and policy decisions more broadly.

Using De-identified Data

The term PII refers to direct identifiers, such as a student's name or address, indirect identifiers, such as a student's date of birth, and any information that is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty. Accordingly, there is no "disclosure" of PII from education records under FERPA, if all direct and indirect identifiers, along with other PII, have been removed.[19]

The Department encourages educational authorities to be aware of publicly available data on students, and of the cumulative effect of student data disclosures. The Department also recognizes that the risk of disclosing identity or individual attributes in statistical information cannot be completely eliminated, at least not without significantly affecting the usefulness of the information. It is critical to manage the risk in each request for information so that data are made available to inform policy and practice, and the risk of disclosure remains very low.

Even if all direct and indirect identifiers have been removed, the remaining data may still allow re-identification of specific individuals. If that is the case, then the information is not considered properly de-identified. Application of additional disclosure avoidance techniques such as masking, blurring, or perturbation may be necessary.[20]

Using Identifiable Data

The most likely exceptions to consent in FERPA that may permit an IDS Lead to redisclose identifiable data are the audit and evaluation and studies exceptions.

The audit and evaluation exception to consent permits disclosures to "authorized representatives" of state and local educational authorities, the Secretary of the U.S. Department of Education, the Attorney General of the United States, and the Comptroller General of the United States. This disclosure must be in connection with either (1) an audit or evaluation of federal- or state-supported education programs, or (2) the enforcement of or compliance with federal legal requirements that relate to those programs.

A government agency or an outside organization may initiate the request to the IDS Lead for data for an audit or evaluation. The IDS Lead may redisclose PII from education records in response to that request if (1) the educational authority has authorized the IDS Lead to make the redisclosure; (2) the redisclosure otherwise complies with FERPA (such as if the redisclosure is to another authorized representative of the educational authority) and with any other applicable federal and state confidentiality and privacy laws; (3) the redisclosure is in connection with an audit or evaluation of a federal- or state-supported education program as defined under FERPA; and, (4) the redisclosure is recorded in compliance with FERPA. The audit or evaluation can be of the federal- or state-supported

[19] See 34 CFR § 99.31(b)(1).

[20] The Privacy Technical Assistance Center's *FAQs on Disclosure Avoidance*, available at https://studentprivacy.ed.gov/resources/frequently-asked-questions-disclosure-avoidance, may be helpful in this regard.

education program in its entirety or of a subset of the population participating in the federal- or state-supported education program in which the researcher has a particular interest.[21]

Examples of projects that may be acceptable under the audit and evaluation exception:

- A state educational agency and statewide Child Welfare agency are interested in assessing whether children in foster care are receiving the necessary supports under state-supported education programs.

- A local human services agency and school district are interested in evaluating the impact of participation in federal- and state-supported early childhood education programs on kindergarten readiness.

- A school district's superintendent is interested in evaluating the effectiveness of state-supported education programs for at-risk students, specifically looking at attendance outcomes. The first project she requests is to evaluate the school district's transportation program (a state-supported education program) to see how effectively it is serving students in assisted housing.

Example of a project that is likely to be unacceptable under the audit and evaluation exception:

- A city housing authority wants to evaluate a program to provide stable housing to families experiencing homelessness using a number of criteria including educational attainment. As stated, the housing authority's program is not a federal- or state-supported education program under FERPA. While the audit and evaluation exception does not apply, the city housing authority could consider obtaining consent from the parents of participating students or requesting aggregate, de-identified data from the school district.

Possible governance models to release PII from education records under the audit and evaluation exception are discussed below. Regardless of the governance structure, every release must meet all criteria to comply with the exception as established in the FERPA regulations.

Criteria to Comply with the Audit and Evaluation Exception

Under this exception, the state or local educational authority must do all of the following: (a) designate the IDS Lead as its "authorized representative," (b) enter into a written agreement with the IDS Lead with required clauses, (c) use reasonable methods to ensure to the greatest extent practicable that its authorized representative uses, protects, and destroys the PII from education records in compliance with FERPA's requirements, and (d) ensure that a record of each request for access to and each disclosure of PII from education records is maintained in compliance with FERPA.[22]

---

[21] Please note that this guidance is specific to the release of student education records in accordance with FERPA. When the request includes the release of other types of data, the protections regarding use and disclosure of those data should also be independently reviewed under applicable law.

[22] See 34 CFR §§ 99.32 and 99.35. Additional details can be found in *Guidance for Reasonable Methods and Written Agreements*, available at https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements.

Some research may also be permissible under FERPA's studies exception to consent.[23] The studies exception applies to an organization (which can be a federal, state, and local agency or an independent organization) conducting studies for, or on behalf of, the school or school district to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. There are a number of other requirements in the FERPA regulations that must be met in order to disclose PII from eduation records without consent to an organization under the studies exception. These include, but are not limited to, that there must be a written agreement with the organization with required clauses and the disclosure must be recorded.[24]

A note on privacy protections for PII on individuals with disabilities…

While the focus of this guidance is FERPA, the Individuals with Disabilities Act (IDEA) regulations incorporate many of the confidentiality provisions of, and applicable exceptions under, FERPA, along with additional provisions. If a student whose PII is subject to FERPA also is referred to, eligible for, or receives services under, either Part C or Part B of the IDEA, any disclosures of PII regarding that student must comply with the applicable confidentiality regulations in Part C or Part B of the IDEA in addition to the requirements identified in this document.

About IDEA

The confidentiality provisions in the IDEA Part B regulations[25] apply to children with disabilities age three through 21 who are referred to, eligible for, or receive services under, Part B of the IDEA. The confidentiality provisions in the IDEA Part C regulations[26] apply to infants and toddlers with disabilities, from birth to age three (and at the state's option until the child enters kindergarten), who are referred to, eligible for, or receive services under, Part C of the IDEA. The IDEA Part B and Part C regulations are two separate sets of regulations and both contain confidentiality provisions that protect the PII collected, maintained, or used under Part B and Part C of the IDEA, respectively. Generally, under both sets of regulations, parental consent is required prior to disclosing PII unless a specific narrowly tailored exception applies.

IDEA and Integrated Data Systems

While IDS participation for an entity with IDEA protected data is similar to the two-stage legal framework to comply with FERPA described in this document, there are additional key differences between the FERPA, and the privacy protections under the IDEA Part B and IDEA Part C regulations. While the audit and evaluation and school official exceptions to consent are applicable to IDEA protected data, there are differences in whether and how they may apply. Additional differences under IDEA are the child find referral exceptions when a child transitions from Part C to Part B of the IDEA as well as the definition of a participating agency under both IDEA Part B and C regulations. Another key difference for IDEA protected data is the requirement for data destruction. This FERPA-related guidance may be a good starting point to approach integrating IDEA protected data into an IDS, but educational authorities should consult with the U.S. Department of Education's Office of Special Education Programs (or OSEP, which administers the IDEA) to identify all criteria to comply with IDEA Part B and/or Part C regulations in the IDS context. Please see the *Additional Resources* section of this guidance for the U.S. Department of Education's cross-walk of FERPA and the IDEA Part B and Part C regulations and other relevant resources.

---

[23] See 20 U.S.C. § 1232g(b)(1)(F); 34 CFR § 99.31(a)(6).

[24] Additional information on both the audit and evaluation and studies exceptions can be found in PTAC's *FERPA Exceptions – Summary*, available at https://studentprivacy.ed.gov/resources/ferpa-exceptions-summary-large-format-11-x-17.

[25] See 34 CFR part 300.

[26] See 34 CFR part 303.

Governance Models For Data Use

There are several ways that an educational authority can structure a governance model to work with an IDS. They fall along a continuum, with the educational authority maintaining the highest level of control on one end to the highest level of delegation on the other. The educational authority should choose an appropriate place on the continuum for (1) internal data analytics, referring to the IDS Lead's access to and use of data and (2) redisclosures, referring to other stakeholders' (government agencies, universities, research organizations, etc.) access to and use of data.

Internal Data Analytics: IDS Lead's Access to and Use of Data

Many stakeholder requests for information can be fulfilled by providing truly de-identified data in the form of aggregate/summarized results or individual-level datasets that do not disclose PII from education records under FERPA. It is important to note, however, that one of the IDS Lead staff members will need to access the raw (likely identifiable) data in order to produce those de-identified results. There are several ways to set up their authorization to do so.

To maintain the highest level of control, the educational authority can require a new written agreement with the IDS Lead for every use of data. Or, if the educational authority is comfortable with more delegation, it can develop one or more written agreements up front that specify a broader research agenda. These agreements would list the most important research questions that are permissible under the audit and evaluation exception (or, in appropriate cases, the school official or studies exceptions) and allow the IDS Lead to access and use data that fit within the defined research agenda for the term of the written agreement. New written agreements would only be required if a research need arises that is outside of the scope of the current research agenda. Please note that if the educational authority is a school district and the IDS Lead is a designated school official, then the research agenda could extend beyond evaluations that are permitted under the audit and evaluation exception so long as the research agenda is part of the research that the school district would otherwise conduct for itself and the school district determines that the research meets its criteria as being for a "legitimate educational interest." In governance structures in which a written agreement is not required for each use of data, the educational authority can increase its control and oversight by incorporating a formal approval structure for data uses in the governance structure. The approval structure can include both approvals to conduct the analysis and approvals of the final results/output before it is made public to ensure that no PII from education records is released.

Redisclosures: Other Stakeholders' Access to and Use of Data

As described above, stakeholders' requests for information can often be fulfilled by the IDS Lead sharing de-identified data. If the request cannot be fulfilled with de-identified data, the IDS Lead may only redisclose PII from education records to an external entity in limited situations in which the project falls under one of FERPA's exceptions to consent and all criteria to comply with FERPA are met. The governance model alternatives range from not permitting any redisclosures, to requiring a new written agreement (between the educational authority and the stakeholder requesting data) for every redisclosure, to allowing redisclosure under the existing agreements the educational authority has with the IDS Lead and the other stakeholders. In governance structures in which a written agreement is not required for each use of data, the educational authority can increase its control and oversight by incorporating a formal approval structure for data uses in the governance structure. The approval structure can include both approvals to conduct the analysis and approvals of the output before it is shared with the stakeholder requesting the data.

The options for governance structures are illustrated below. The educational authority should decide which alternative makes sense in the local context for both the internal data analytics and for evaluations and analyses requiring redisclosure.

Most Control	***INTERNAL DATA ANALYTICS*** *IDS Lead Data Access & Use*	***REDISCLOSURES*** *Other Stakeholders' Access to Identified Data*
		A **No permitted redisclosures** of identifiable integrated data.
	1 New, **project-specific written agreements** are required for each data use.	B **Redisclosures are permitted with new, project-specific written agreements** between the educational authority and the stakeholder requesting data. The IDS Lead serves only as the agent to provide data.
	2 Set up **broad initial written agreement(s)** with key research questions. A **formal approval from the educational authority** is required for each data use. The educational authority reviews each proposed use of data to determine if it is consistent with FERPA and other applicable federal and state privacy and confidentiality laws.	C **Redisclosures are permitted under existing broad written agreement(s)** between the educational authority and the IDS Lead, as well as a written agreement between the IDS Lead and the stakeholder requesting data. A **formal approval from the educational authority is required for** each redisclosure.
	3 Set up **broad initial written agreement(s)** with key research questions. The IDS Lead provides a **notification to the educational authority** of each data use that fits under the existing broad written agreement(s).	D **Redisclosures are permitted under existing broad written agreement(s)** between the educational authority and the IDS Lead, as well as a written agreement between the IDS Lead and the stakeholder requesting data. The IDS Lead provides a **notification to the educational authority** of each redisclosure.
Most Dele-gation		

The following scenarios describe IDS implementations in more detail. The scenarios identify the educational authority and IDS Lead, the legal framework they used to develop the partnership, and the data use and governance models they have set up.

SCENARIO 1

Educational Authority	*IDS Lead*
City School District	University Research Team

Legal framework to partner

A local city school district designated a university research team as a school official to provide the district with research and evaluation with a focus on cross-agency data integration. The district entered into a written agreement with a three-year term that specifies all of the acceptable uses of the city school district's data as well as the governance structure that must be followed. Additionally, the district included clear and detailed information in its annual FERPA notice to parents and eligible students in the district that describes how the research constitutes a legitimate educational interest and that the university research team is serving as a school official.

Data use and governance model

The university research team (IDS Lead) supports the research and evaluation needs of its school district partners and also makes de-identified, integrated data available to the public. For example, the IDS Lead prepares community profiles that present a number of indicators for neighborhoods across the county including property values, crime rates, and educational outcomes.

The governance structure chosen allows only researchers at the IDS Lead agency to access PII for research and evaluation purposes. The IDS Lead must obtain a formal approval from the district for every use of the data prior to starting the project. To secure the approval, the IDS Lead sends the district a description of the project, the specific data elements that the IDS Lead will access, a description of the final product, and a list of the parties with which the IDS Lead will share the de-identified results. In some cases the school district approves the project but requires an additional review and approval of the final product before it is disseminated. No redisclosures of identifiable data are permissible at this time. All access to PII from education records to conduct analysis is restricted to staff of the IDS Lead.

In the illustration of governance model alternatives, this framework aligns to IDS Lead access 2 and other stakeholders' access A.

SCENARIO 2

Educational Authority	*IDS Lead*
State Educational Agency (SEA)	State Health & Human Services Agency (HHS)

Legal framework to partner

The SEA that runs the statewide longitudinal data system (SLDS) partners with the state HHS agency through FERPA's audit and evaluation exception. The SEA entered into a formal written agreement with a two-year term that designates the state's HHS agency as the authorized representative of the SEA to audit and evaluate federal- and state-supported education programs by making critical cross-agency outcome data available. In the agreement, their research agenda is set forth through several broadly defined research questions. Their research priorities include the audit and evaluation of federal- and state-supported education programs for the state's most vulnerable students (e.g., students with physical and mental health issues, students living in poverty, and students involved in the juvenile justice system), as well as looking at trends in academic performance by neighborhood and identifying which neighborhood-level indicators may be predictive of academic success or challenges.

Data use and governance model

The SEA sends PII from education records to the state HHS agency every 45 days. Analysts at the state HHS agency have access to the PII to conduct research and evaluation that fits under one of the specified research questions. For each use of data, the state HHS agency provides a notice to staff at the SEA when a project begins and again to share the results once it is completed.

The IDS Lead (state HHS agency) is also the agent to share identifiable, individual-level integrated data with outside researchers in limited cases. The IDS Lead only rediscloses PII from education records if each agency that "owns" the PII being requested enters into a formal, written agreement with the entity requesting data and records that redisclosure. If PII from education records is being requested, the written agreement includes all the required information to comply with FERPA's audit and evaluation exception and names the state HHS agency as the party to provide the integrated data.

In the illustration of governance model alternatives this framework aligns to IDS Lead access 3 and other stakeholders' access B.

SCENARIO 3

Educational Authority	*IDS Lead*
Multiple School Districts	County Department of Social Services (DSS)

Legal framework to partner

Ten local school districts have separately designated the county DSS as their school official to conduct research and analytics on their behalf. DSS entered into a written agreement with each school district for a three-year term that specifies all of the acceptable uses for data as well as the governance structure that must be followed. Additionally, the school districts included clear and detailed information in their annual FERPA notices to parents and eligible students in the district that described DSS as a school official and indicated that conducting research and analytics serve legitimate educational interests.

Data use and governance model

School districts send DSS PII from education records every week through a Secure File Transfer Protocol (SFTP). The research team at DSS accesses the PII to support the research and evaluation needs of its school district partners as well as other stakeholders in the community. DSS and the districts are particularly interested in improving the school districts' federal- and state-supported education programs for children involved in human services (e.g., child welfare, homeless and housing supports, mental health services). The research and evaluation team at DSS conducts research and evaluations and shares aggregate, de-identified results with school district partners and other stakeholders in the community. Research and evaluation is used to inform collaborative, data driven strategies throughout the county.

The IDS Lead (DSS) provides a notice to the school districts when their data are used. Additionally, if DSS intends to make any of the findings public, then the school district partners review and approve the reports. DSS is also the agent to share individual-level integrated data with outside researchers. If a researcher is interested in de-identified student-level data, then the researcher must write a formal memorandum to the districts' administration with a description of their project and the specific data from education records that the researcher is requesting. The de-identified data may be shared with the outside researcher if approved by the district. If the outside researcher is requesting identifiable data, the disclosure would only be permissible under FERPA if the researcher requesting the PII enters into a separate agreement with each of the school districts whose data will be used under an applicable exception to consent. If approved by the districts' leadership, then DSS is the agent to securely share that PII with the researcher. Both DSS and its school district partners record the redisclosures.

In the illustration of governance model alternatives this framework aligns to IDS Lead access 3 and other stakeholders' access B.

Best Practices

Transparency

Transparency is important at every stage of IDS participation. The educational authority and IDS Lead should commit time and resources to ensure all stakeholders are informed. The communication should be multi-layered and accessible to all stakeholders that are affected by the work including, for example, state and local government agencies, policymakers, school staff and administration, and children and families in the community.

A critical message for stakeholders is the value of integrating and using multiple agencies' data. The educational authority and IDS Lead should clearly communicate what value they intend to create through the partnership and then publicize successful use cases of the integrated data throughout the partnership. Stakeholders should be informed on what projects have been completed, what was learned in each, and what program or policy changes resulted.

In addition to understanding the value of the partnerships, stakeholders should be fully informed on the mechanics of the partnership, including what data are being shared, who has access to it, and what data governance and information security programs are in place to protect student privacy.

Lastly, the educational authority and IDS Lead should develop methods to collect feedback from stakeholders to ensure their voices are heard and that their feedback informs the future work of the IDS.

Governance and Information Security

While agencies that partner with an IDS likely have established governance and information security programs within their organization, it is important to also develop a multi-agency governance and information security program for IDS participants.[27] Governance and information security program elements that are most relevant to an IDS are highlighted below.

- ☑ **Decisionmaking authority** – Assigning appropriate levels of authority to data stewards and proactively defining the scope and limitations of that authority.
- ☑ **Standard policies and procedures** – Adopting and enforcing clear policies and procedures in a written data stewardship plan is necessary to ensure that everyone in the organization understands the importance of data quality and security – and that staff are motivated and empowered to implement data governance.
- ☑ **Data content management** – Closely managing data content, including identifying the purposes for which data are collected, is necessary to justify the collection of sensitive data, optimize data management processes, and ensure compliance with federal, state, and local laws.
- ☑ **Data records management** – Specifying appropriate managerial and user activities related to handling data is necessary to provide data stewards and users with appropriate tools for complying with an organization's security policies. Has the organization established and

[27] A full checklist of best practices in data governance can be found in PTAC's *Data Governance Checklist*, available at https://studentprivacy.ed.gov/resources/checklist-data-governance.

communicated policies and procedures for handling records throughout all stages of the data lifecycle, including acquiring, maintaining, using, and archiving or destroying data?

☑ **Data quality** – Ensuring that data are accurate, relevant, timely, and complete for the purposes they are intended to be used is a high-priority issue for any organization. The key to maintaining high-quality data is a proactive approach to data governance that requires establishing and regularly updating strategies for preventing, detecting, and correcting errors and misuses of data.

☑ **Data access** – Defining and assigning differentiated levels of data access to individuals based on their roles and responsibilities in the organization is critical to preventing unauthorized access and minimizing the risk of data breaches.

☑ **Recordation** – Maintaining a record of each request for access to, and each disclosure of PII from education records of each student is critical. The record of disclosure should cover both the releases of PII from the educational authority to the IDS Lead as well as the redisclosures from the IDS Lead to other stakeholders.

☑ **Data security and risk management** – Ensuring the security of sensitive and personally identifiable data and mitigating the risks of unauthorized disclosure of these data is a top priority for an effective data governance plan.[28] Important components of a data security program for an IDS include, but are not limited to, physical security, network mapping, authentication, layered defense architecture, secure configurations, access controls, firewalls and intrusion detection/prevention systems, automated vulnerability scanning, patch management, incident handling, and audit and compliance monitoring.

[28] See PTAC's *Data Security Checklist*, available at https://studentprivacy.ed.gov/resources/data-security-checklist, for additional information on essential components that should be considered when building a data security program.

One-Page Summary of FERPA Compliance

<table>
<tr><th></th><th></th><th>AUDIT & EVALUATION EXCEPTION (for Stage 1)
Usable by school districts, other local educational authorities, and state educational authorities</th><th>SCHOOL OFFICIAL EXCEPTION (for Stage 1)
Usable by school districts</th></tr>
<tr><td>STAGE 1: Becoming an IDS Partner</td><td>CREATING AN INTEGRATED DATA INFRASTRUCTURE
IDS Lead collects PII from education records and links with other IDS data sources in an access-controlled environment for future use</td><td>State and local educational authorities are permitted to create an integrated data infrastructure through an IDS using the audit and evaluation exception. The specific purpose for which the PII from education records is redisclosed to the IDS Lead under this exception, is to facilitate future audits and evaluations of federal- or state-supported education programs by establishing linked data. All other criteria to comply with the audit and evaluation exception must be met including written agreement with the IDS Lead and ensuring to the greatest extent practicable that the IDS Lead uses, protects, and destroys the PII from education records in compliance with FERPA.

Please refer to page 7 of this guidance document to see the full list of criteria to comply with the audit and evaluation exception.</td><td>This is permissible if the IDS Lead is performing a function for which the school district would otherwise use its own employees and meets all other criteria to comply with the school official exception. In the case of an IDS, the IDS Lead may perform, for the district, the function of creating an integrated data infrastructure, including linking education data with other IDS data sources, maintaining security, and controlling access to the data.

Please refer to page 9 to see the full list of criteria to comply with the school official exception.</td></tr>
<tr><td rowspan="3">STAGE 2: Approving the Use of Integrated Data</td><td rowspan="2">INTERNAL DATA ANALYTICS
Staff of the IDS Lead accesses individual-level data to conduct analysis.</td><td>Staff of the IDS Lead may use the linked data internally to conduct analysis <u>if</u> it is a data analysis project (project) to audit or evaluate a federal- or state-supported education program. If the project aligns to an audit or evaluation that was named in the written agreement to create the integrated data infrastructure, then it may be conducted by staff of the IDS Lead under the existing agreement. If the project is not listed in the initial written agreement, but still aligns to an audit or evaluation of a federal- or state-supported education program, then the IDS Lead can enter into an additional written agreement with the educational entity disclosing the data (state educational authority or school district) to access linked data for the project.</td><td>Staff of the IDS Lead may use the linked data internally to conduct analysis if it is a project that the school district would otherwise conduct itself. To ensure that this is the case, the project request should come from the school district or be formally approved by the school district. The school district may approve requests either on a project-specific basis or by generating a list of pre-approved types of projects that may be conducted by staff of the IDS Lead.</td></tr>
<tr><td colspan="2">Under both exceptions, for internal data analytics, the access to linked data is limited to staff of the IDS Lead. No individuals outside the IDS Lead have access to PII from education records. Therefore, no additional disclosures take place. The results of the internal analysis may only be shared with external entities in non-identifiable formats (de-identified aggregate or individual-level data). The IDS Lead may share PII from education records back with the educational entity that originally disclosed the PII from education records.</td></tr>
<tr><td>REDISCLOSURE
IDS Lead re-discloses individual-level data to an external entity</td><td colspan="2">Under both exceptions, the IDS Lead may only redisclose PII from education records without consent to an external entity in limited situations when the project falls under the audit and evaluation or studies exception and all criteria to comply are met. In most cases, the written agreements will be with the educational entity disclosing data to the IDS Lead and the external entity requesting data, with the IDS Lead named as the party to redisclose the data. FERPA's recordation provisions also must be met for the IDS Lead to redisclose PII from education records to an external entity.</td></tr>
<tr><td colspan="2">ACCESS TO INDIVIDUAL RECORDS FOR SERVICE DELIVERY
IDS Lead and partner agencies accessing identifiable records to support service delivery</td><td colspan="2">In most cases, the exceptions to consent used to operate an IDS will not permit use of PII from education records for the delivery of services. For example, the IDS Lead may not permit staff at a public housing community to access PII from education records for their clients under the exceptions used to participate in an IDS.

This guidance is focused on using an IDS for research and evaluation purposes. Please note that service workers may be able to access PII from education records through the IDS if they have obtained prior written consent or have legal authority to access the records without consent. For example, the Uninterrupted Scholars Act permits child welfare caseworkers with the right to access a student's case plan, as defined and determined by the state or tribal organization, to access, without prior written consent, education records for children in foster care when the child welfare agency they represent is "legally responsible, in accordance with state or tribal law, for the care and protection of the student." If the IDS Lead is an agent to permit this access (where legal), the governance structure to permit this access should be documented in the written agreement/contract between the educational authority and IDS Lead.</td></tr>
</table>

Additional Resources

Websites

DaSy Center: http://dasycenter.org/

U.S. Department of Education, Family Policy Compliance Office (FPCO): https://studentprivacy.ed.gov/

U.S. Department of Education, Office of Special Education Programs (OSEP): http://www2.ed.gov/about/offices/list/osers/osep/index.html

U.S. Department of Education, Privacy Technical Assistance Center (PTAC): https://studentprivacy.ed.gov

U.S. Department of Education, Privacy Technical Assistance Center (PTAC), Early Childhood Resources: https://studentprivacy.ed.gov/audience/early-childhood-educators

Documents

U.S. Department of Education (2012): *IDEA and FERPA Confidentiality Provisions,* available at https://studentprivacy.ed.gov/training/insersection-ferpa-and-idea-confidentiality-provisions-march-2012.

U.S. Department of Education, National Center for Education Statistics (2012): *Centralized vs. Federated: State Approaches to P-20W Data System,* available at http://nces.ed.gov/programs/slds/pdf/federated_centralized_print.pdf.

U.S. Department of Education, National Center for Education Statistics (2011): *SLDS Technical Brief 2: Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records* (NCES 2011-602), available at http://nces.ed.gov/pubs2011/2011602.pdf.

U.S. Department of Education, Office of Special Education Programs (2016): *FAQ on Early Childhood Privacy and Confidentiality,* available at http://www2.ed.gov/policy/speced/guid/idea/memosdcltrs/idea-confidentiality-requirements-faq.pdf.

U.S. Department of Education, Privacy Technical Assistance Center (2012, updated 2015): *Case Study #5: Minimizing Access to PII: Best Practices for Access Controls and Disclosure Avoidance Techniques, available at* https://studentprivacy.ed.gov/resources/case-study-5-minimizing-pii-access.

U.S. Department of Education, Privacy Technical Assistance Center (2011): *Checklist: Data Governance,* available at https://studentprivacy.ed.gov/resources/checklist-data-governance.

U.S. Department of Education, Privacy Technical Assistance Center (2011, updated 2015): *Checklist: Data Security,* available at https://studentprivacy.ed.gov/resources/data-security-checklist.

U.S. Department of Education, Privacy Technical Assistance Center (2012, updated 2013): *Written Agreement Checklist,* available at https://studentprivacy.ed.gov/resources/written-agreement-checklist

U.S. Department of Education, Privacy Technical Assistance Center (2011): *Data Governance and Stewardship*, available at https://studentprivacy.ed.gov/resources/issue-brief-data-governance-and-stewardship.

U.S. Department of Education, Privacy Technical Assistance Center (2011): *Data Security: Top Threats to Data Protection*, available at https://studentprivacy.ed.gov/resources/issue-brief-data-security-top-threats-data-protection.

U.S. Department of Education, Privacy Technical Assistance Center (2014): *FERPA Exceptions Summary*, available at https://studentprivacy.ed.gov/resources/ferpa-exceptions-summary-large-format-11-x-17.

U.S. Department of Education, Privacy Technical Assistance Center (2013, updated 2015): *Guidance for Reasonable Methods and Written Agreements*, available at https://studentprivacy.ed.gov/resources/guidance-reasonable-methods-and-written-agreements.

U.S. Department of Health and Human Services and the U.S. Department of Education (2016): *The Integration of Early Childhood Data*, available at https://www.acf.hhs.gov/sites/default/files/ecd/intergration_of_early_childhood_data_final.pdf