FPF Student Privacy Train-the-Trainer Program Module 4: Sharing Data CLE Materials

June 18, 2020

Module 4: Sharing Data

June 18, 2020

TABLE OF CONTENTS

Note: CLE materials are provided digitally; attendees may receive a printed version of the materials upon request.

Homework/Asynchronous Activities

There are three individual activities for this module.

1. Find the Right FERPA Exception
2. T-Chart: Studies Versus Audit and Evaluation Exceptions
3. Floor-to-Ceiling: Best Practices for Written Agreements

Please complete the activities in this document and email the document to ttt@fpf.org by **June 12th**.

1. Review PTAC's FERPA Exception Chart and FPF's FERPA Permitted Data Sharing Chart. Determine the appropriate exception for the following scenarios.

    a. **Scenario 1:** The state education agency (SEA) in State Pretend participates in the State Fiscal Stabilization Fund (SFSF) program. By accepting funds under the SFSF program, the SEA agreed to collect and publish various data, including data on students' success in college (such as whether they enrolled in remedial courses). The SEA has data on State Pretend high school graduates because it has a functioning K-12 statewide longitudinal data system (SLDS) and wants to provide its high schools with information on how their graduates are doing at the postsecondary level. To prepare the feedback reports, however, the SEA needs to match data on State Pretend's public high school graduates with data from State Pretend's public institutions of higher education (IHEs). The SEA wishes to obtain these data yearly, and house the data in its SLDS so that it can conduct an ongoing evaluation and produce annual individual high school feedback reports.

    b. **Scenario 2:** Anywhere District has a new superintendent that believes strongly in data-driven decision making. After a long arduous request for proposal (RFP) process, information technology staff have chosen a data warehouse and dashboard product. This warehouse will contain all data collected and calculated for all schools in the district.

2. Read [The Family Educational Rights and Privacy Act: Guidance for Reasonable Methods and Written Agreements].

    a. Use a T-chart labeled “Same” and “Different” to illustrate the similarities and differences between the studies and audit/evaluation exceptions.

    b. The article stated that FERPA is the “floor as opposed to the ceiling” when it comes to protecting privacy.

        i. Create a vertical continuum. Label the top of the continuum “ceiling” and the bottom of the continuum “floor.”

        ii. Indicate which of the 15 best practices for written agreements included in the above article are closer to the floor and which are closer to the ceiling, by placing them on this image.

FERPA Permitted Data Sharing Chart

Aside from parental consent and directory information, the two most common FERPA exceptions, there are a number of other circumstances when prior consent is not required to disclose information about a student.

The following are categories of people/organizations that may not need express student consent to gain access to certain information about students.

Individual/Entity Seeking Information:		**Type of Information Available Without Consent…**
Parents	Of Dependent Post-Secondary Students	Generally – any student information
	Of Non-Dependent Post-Secondary Students	Information in connection with the student's health or safety
		Information related to the student's violation of the law or the academic institution's policy governing the use or possession of alcohol or controlled substances.
Schools		In which the student intends to enroll (often called the "**school official** exception")
Financial Aid Offices		Facts relevant to determining a student's eligibility, amount, or conditions surrounding receiving financial aid
Authorized Representative of Federal, State, and Local Governments and Educational Authorities		Auditing, evaluating, or enforcing education programs (often called the "**audit and evaluation** exception")
Organizations		Data used to conduct studies, predictive tests, administering student aid program, or improving instruction (often called the "**studies** exception")
Judicial or Law Enforcement Authority		In compliance with an order or subpoena
Victims		Results of a disciplinary hearing of a crime of violence
Third Parties		Final results of a disciplinary hearing concerning a student who is an alleged perpetrator of a crime of violence and who was found to have committed a violation of the institution's rules or policies
Community Notification Program		Information concerning a student required to register as a sex offender in the State

FUTURE OF PRIVACY FORUM

TRAIN THE TRAINER

MODULE 4 WEBINAR

PD FOR EDUCATORS

MODULE 4 OBJECTIVES

1. Compare and contrast FERPA exceptions.
2. Select the correct exception for various situations.
3. Identify FERPA required elements of a data sharing agreement and recommended elements.
4. Locate resources to assist in drafting data sharing agreements.

ACTION PLAN AND TRAINING CHECK IN

Action Plan

1. Create an online space to build your portfolio.
2. Begin collecting resources and tools.

Presentations

1. Get prepared.
2. Look for places to present or train.
3. Build your portfolio.

MODULE 4 ACTIVITIES

FIND THE RIGHT FERPA EXCEPTION

Scenario 1

The state education agency (SEA) in State Pretend participates in the State Fiscal Stabilization Fund (SFSF) program. By accepting funds under the SFSF program, the SEA agreed to collect and publish various data, including data on students' success in college (such as whether they enrolled in remedial courses). The SEA has data on State Pretend high school graduates because it has a functioning K-12 statewide longitudinal data system (SLDS) and wants to provide its high schools with information on how their graduates are doing at the postsecondary level. To prepare the feedback reports, however, the SEA needs to match data on State Pretend's public high school graduates with data from State Pretend's public institutions of higher education (IHEs). The SEA wishes to obtain these data yearly, and house the data in its SLDS so that it can conduct an ongoing evaluation and produce annual individual high school feedback reports.

MODULE 4 ACTIVITIES

FIND THE RIGHT FERPA EXCEPTION

FUTURE OF PRIVACY FORUM
TRAIN THE TRAINER

AUDIT OR EVALUATION EXCEPTION

Scenario 1

The state education agency (SEA) in State Pretend participates in the State Fiscal Stabilization Fund (SFSF) program. By accepting funds under the SFSF program, the SEA agreed to collect and publish various data, including data on students' success in college (such as whether they enrolled in remedial courses). The SEA has data on State Pretend high school graduates because it has a functioning K-12 statewide longitudinal data system (SLDS) and wants to provide its high schools with information on how their graduates are doing at the postsecondary level. To prepare the feedback reports, however, the SEA needs to match data on State Pretend's public high school graduates with data from State Pretend's public institutions of higher education (IHEs). The SEA wishes to obtain these data yearly, and house the data in its SLDS so that it can conduct an ongoing evaluation and produce annual individual high school feedback reports.

MODULE 4 ACTIVITIES

FIND THE RIGHT FERPA EXCEPTION

Scenario 2

Anywhere District has a new superintendent that believes strongly in data-driven decision making. After a long arduous request for proposal (RFP) process, information technology staff have chosen a data warehouse and dashboard product. This warehouse will contain all data collected and calculated for all schools in the district.

MODULE 4 ACTIVITIES

FIND THE RIGHT FERPA EXCEPTION

SCHOOL OFFICIAL EXCEPTION

Scenario 2

Anywhere District has a new superintendent that believes strongly in data-driven decision making. After a long arduous request for proposal (RFP) process, information technology staff have chosen a data warehouse and dashboard product. This warehouse will contain all data collected and calculated for all schools in the district.

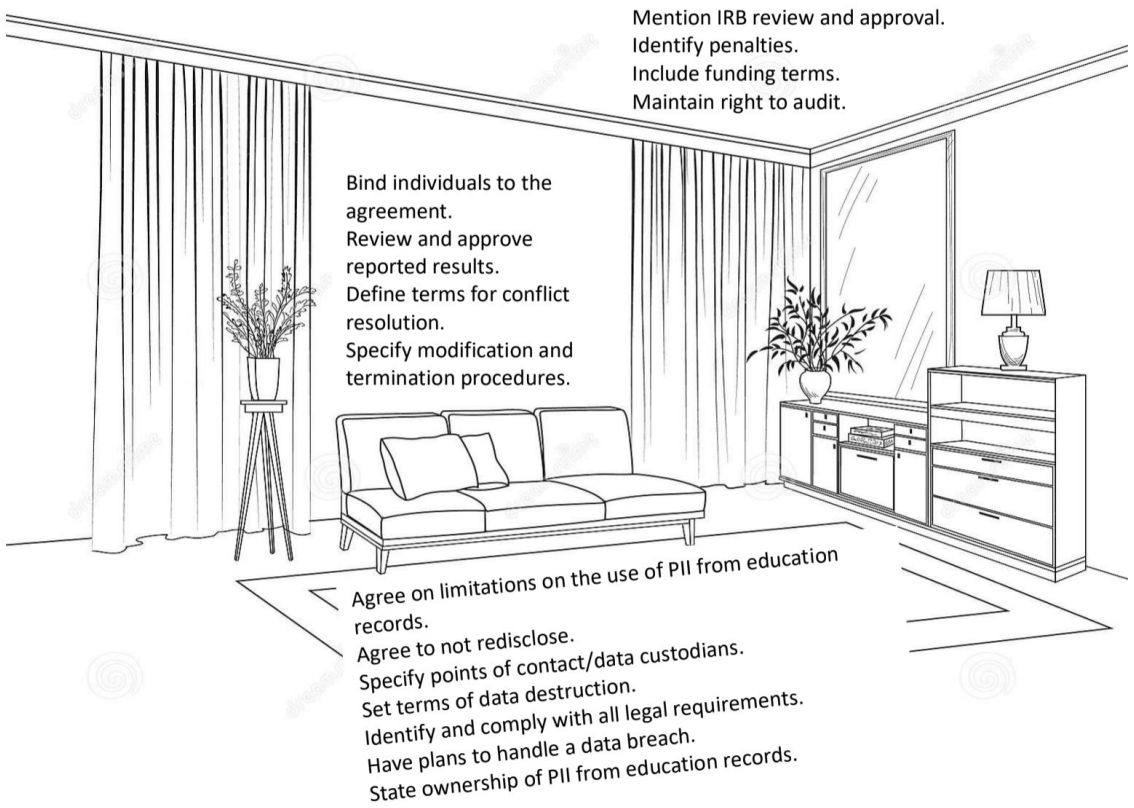
MODULE 4 ACTIVITIES

T-CHART: STUDIES VS AUDIT AND EVALUATION

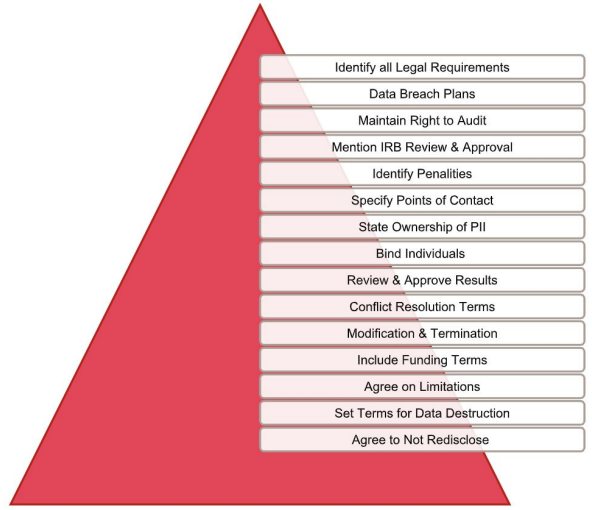
SAME	DIFFERENT
Allows for disclosure of PII without prior written consent from parents/eligible students	Uses • Studies - Purpose of conducting studies for, or on behalf of, schools • Audit/Evaluation - Purpose of auditing/evaluating a federal or state supported education program
Requires written agreement when disclosing PII	Written Agreements • Audit/Evaluation - Designate individual/entity as authorized representative; state disclosure of PII is for audit, evaluation, or enforcement/compliance; include methodology
Published results must protect confidentiality and privacy of individuals	
Requires destruction of PII when no longer needed or as specified in agreement	Under audit and evaluation, must take additional steps (“reasonable methods”) to ensure that the authorized representative is FERPA-compliant

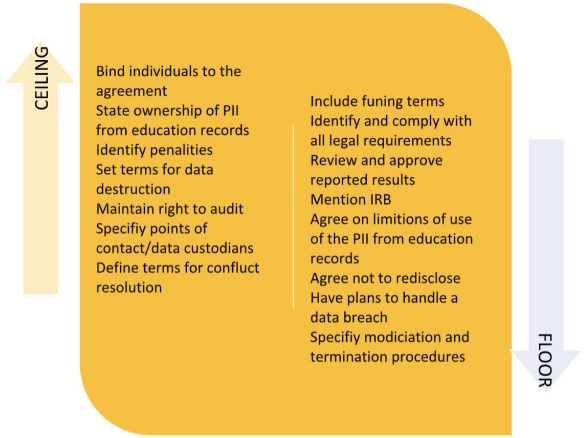
MODULE 4 ACTIVITIES

FLOOR-TO-CEILING:
BEST PRACTICES FOR WRITTEN AGREEMENTS



CEILING
Create third-party beneficiary rights, such as allowing parties injured by a data breach to sue for damages.
Require organization to conduct background investigations of employees who will have access to PII from education records, or conduct these investigations yourself.
Binding individuals to an agreement: identify the individuals in the agreement itself, and have them execute the agreement in their individual capacity.
Public posting of all data share agreements.
IRB Review: If IRB review and approval is required or expected, this may be noted in the written agreement.
In the absence of a quality training program for employees, train the organization's employees yourself.
In the agreements, require individuals accessing the PII from education records to execute affidavits of nondisclosure or other documentation indicating their individual agreement to handle the PII from education records properly.
Include penalties under state contract law such as liquidated damages, data bans of varying length, and any other penalties the parties to the agreement deem appropriate
Require organization to disclose past FERPA or data management violations. If you discover past violations, explore the circumstances behind the violation
Include a method for documenting the destruction, such as the use of notarized statements
Require detailed data breach plan, including specific procedures detailing the parties' expectations in the event that PII is lost or improperly disclosed, including specifying the parties' responsibilities with regard to breach response and notification and financial responsibility
Review and approve results of study/audit/evaluation
Clearly define destruction process
Clearly define the terms for conflict resolution
Maintain right to audit
Maintain ownership of PII
Require compliance with all applicable Federal, state, and local laws and regulations, and identify the legal authority that permits the audit, evaluation, or enforcement or compliance activity.
Specify points of contact and data custodians
Convey Limits on use of PII—that it can only be used for the activities described in the agreement. The agreement may also address methodological limitations.
Disclose only PII necessary for conducting study/audit/evaluation
Specify how agreement can be modified or terminated.
Verify existence of disciplinary policies for employees that violate FERPA
Verify existence of sound data security plan
Verify data stewardship program
Verify training for employees
Obtain assurances against redisclosure
FLOOR





PRESENTATION

Mark Williams
Partner, Co-Chair
eMatters & Higher Education
Practice Groups
Fagen Friedman & Fulfrost LLP (F3)

Lori Chiu
Associate, Co-Chair
eMatters Practice Group
Fagen Friedman & Fulfrost LLP (F3)

FUTURE OF PRIVACY FORUM

TRAIN THE TRAINER

Overview

- FERPA Refresher
- Fundamentals of Data Sharing
- Data Sharing Scenarios
    - Parent or Student Consent
    - School Official Exception
    - Research Exception
    - Law Enforcement/Public Safety

FERPA

- Family Educational Rights and Privacy Act (20 U.S.C. §1232g; 34 C.F.R. Part 99)
- Programs Funded by USDOE
- Protects personally identifiable information (“PII”) in pupil records
- “Pupil record”

  (1) Directly relates to identifiable student

  (2) Maintained by an LEA or a party acting on behalf of an LEA

Basic Philosophy of Student Data Sharing

Introduction: FERPA and related student data privacy statutes at the state level should not be viewed as creating a kind of “Lock Box” for student privacy. The law and the functioning of education depends on regular flows of student data to individuals and organizations. Rather FERPA and other statues set “rules of the road” regarding how this data may be shared.

Three Basic Questions for Data Sharing

(1) What is the scope of access (e.g. types of records)?

(2) Who is accessing the records?

(3) What is the purpose of the access?

Types of Student Data Access

Introduction: FERPA and state statutes contain a large number of ways in which student data can be accessed, including audits and reviews by various federal and state agencies. Our review here is restricted to those methods of access are used the most often or have presented the most legal questions from a technological viewpoint.

Example: Student or parent access to student records.

Four “Hot” Areas of Student Data Access

(1) Parent or Student Consent

(2) School Official Exception

(3) Research Exception

(4) Law Enforcement/Public Safety

Student/Parent Consent

- Consent is often considered the “Crown Jewel” of student data access. Why? In what settings does consent work best?

- Consent can also be looked upon as the “Holy Grail” as well as the “Crown Jewel” of student data access, especially in a large setting. Why is that?

- Aiding in the process of student consent, annual notices and vendor facilitation? What are the drawbacks each of approach?

Student/Parent Consent (Cont.)

The key consideration here is ensuring that the consent is informed.

(1) Consent must be in writing;

(2) Specify the records that may be disclosed;

(3) State the purpose of the disclosure; and

(4) Identify the party or class of parties to whom the disclosure may be made.

These key considerations may aid us when we approach other types of access to student data.

Current Issues in the Area of Consent

(1) How long should the consent last? Is it legal or ethical to have a parent consent to access to student data for longitudinal studies that may persist for years or decades?

(2) Can consent be withdrawn and the data deleted? (Analogous CCPA in California affords consumers that right.)

School Official Exception

Introduction: Perhaps the most discussed and employed method by which student data is accessed, especially by outside parties.

To be considered a “School Official” an outside party must:

(1) Perform a service or function which the agency would otherwise perform.

(2) Be under the direct control of the agency or institution with respect to the use and maintenance of education records.

(3) Be subject to the rules governing the use and redisclosure of personally identifiable information from education records.

Ensuring the Purpose and Spirit of the School Official Exception

- The most important piece of the Student Official exception is to take steps so that the data transferred to or processed by a third party is under direct supervision of the school district. This can be quite challenging in cases where the data is stored offsite by often large corporations.

- A contract between the vendor and the school district is universally considered the best way to lay out and formalize this direct supervision.

Three Main Objectives of a Data Privacy Agreement ("DPA")

(1) List the requirements and prohibitions of the applicable law.

(2) Establish a system of oversight and communication between the school district and the vendor, a data relationship over time.

(3) Correlates with your educational community's expectations, i.e. the "digital social compact."

Negotiating a DPA

- **Step One:** Getting the vendor to understand the need for a DPA in the first place (Vendor based DPAs or Online Privacy Policies).
- **Step Two:** Text Revisions or Amendments.
- **Step Three:** The Vendor “Golden Triangle” of Sales, Legal and Engineering departments.
- **Step Four:** Vendors and comfort spots, expect a certain amount of negotiation “messiness”.

Main Current Issues of Negotiation

(1) Security Measures

(2) Data Breach Notifications

(3) Subprocessors

(4) Audits

(5) Advertising

The Rise of Form Data Privacy Agreements

(1) Hidden Commonalities of State and Federal Law.

(2) State Form Agreements and “Exhibit “E”.

(3) Role of Student Data Privacy Consortium (“SDPC”).

(4) Coming Soon: The Standard Student Data Privacy Agreement.

Research Data Agreements

- Research Data Agreements (“RDA”s) are a study in contrast with vendor based “School Official Exception” contracts.

- In the FERPA regulations there are a number of requirements governing research agreements that are not present with School Official sections.

Research Data Agreements (cont.)

Examples include:

(1) Data disposal requirements.

(2) Only authorized use of data.

(3) Specifies the purpose, scope and duration of the study or studies and the information to be disclosed.

(4) Requires a written agreement.

Research Data Agreements (cont.)

- Despite the specificity of the requirements under FERPA and the presumable frequent use of education data by research institutes there are no form agreements.
- Agreements tend to be “one offs”, and poorly worded.
- Why?
- The challenges of Inter-Agency Data Agreements.

Law Enforcement Data Agreements

- FERPA regulations permit disclosure of PII from pupil records when disclosure is necessary to protect the health or safety of the student or other individuals

- Determination on a case-by-case basis
  - Totality of the circumstances pertaining to a threat
  - Articulable and significant threat to the health or safety of a student or other individuals
  - Third party needs PII to protect health or safety

Law Enforcement Data Agreements

- Limited to period of the emergency
- Within reasonable time period, must update pupil record
  - Articulable and significant threat that formed the basis for the disclosure
  - Parties to whom information was disclosed

Law Enforcement Data Agreements

- Data sharing can be facilitated under “health or safety emergency” exception

- Consider whether “school official” exception also applies (example: SROs)

- Review employee collective bargaining agreements to ensure compliance with any requirements and confirm there are no conflicts (example: notice to bargaining units?)

Key Negotiating Points

- Definition of “Emergency Situation”
  - A situation that poses an imminent threat to the life, safety, health, or property of the District, its students, its staff, and other occupants of the District, including but not limited to fire, threatened or actual use of firearms or other potentially deadly or injurious weapons, and health-related emergencies.
- Pupil records vs. law enforcement records
  - Law enforcement records: created by law enforcement unit; created for a law enforcement purpose; maintained by law enforcement unit

Key Negotiating Points (cont.)

- Procedures for access to surveillance system or SIS
  - Maintain access logs
  - Limitations on duration of access
- Access in non-emergency situations
  - Sharing based on parent or eligible student consent
  - Sharing based on “school official” exception
- Indemnification provisions

UPCOMING WEBINARS

MODULE 5: MANAGING THIRD PARTIES

Thursday, July 27th 1-2:30PM ET

Kerry Gallagher, *Assistant Principal for Teaching and Learning*, St. John's Prep, *Director of K-12 Education*, ConnectSafely.org
Girard Kelly, *Senior Counsel & Director*, Privacy Program, Common Sense
Allen Miedema, *Executive Director*, Technology Department, Northshore School District

MODULE 6: SAFEGUARDING DATA SECURITY

TBD

Holly Brady, *Senior Counsel*, *Governance, Compliance and Employment*, Altria Client Services
Tanya Forsheit, *Partner*, *Chair*, *Privacy and Data Security Group*, Frankfurt Kurnit Klein & Selz
Kirk Nahra, *Partner*, Wiley Rein

FERPA Exceptions—Summary

Privacy Technical Assistance Center

This Privacy Technical Assistance Center (PTAC) document is designed to assist State and local educational agencies (SEAs and LEAs) and educational institutions with determining under what conditions the Family Educational Rights and Privacy Act (FERPA) permits the disclosure of personally identifiable information (PII) from education records to third parties, such as researchers, contractors, volunteers, and journalists.

Generally, FERPA requires written consent from parents or "eligible students" (students who are at least 18 years of age or attending a postsecondary institution) in order to release PII from education records. In the absence of the written consent, FERPA permits an educational agency or institution to disclose PII from an education record of a student if the disclosure meets one or more of the conditions outlined in 20 U.S.C. § 1232g(b) and (h) – (j) and 34 CFR § 99.31. Below is a high-level overview of the four most commonly used exceptions to the FERPA written consent requirement, including applicable recordation requirements. For a more detailed explanation of these and other FERPA exceptions, please visit http://ptac.ed.gov.

Directory Information*	School Official (Schools and LEAs only)	Studies	Audit or Evaluation
Conditions that must be met			
1. A school and/or LEA must properly designate "directory information": a. Directory information may only include PII that is generally not considered harmful or an invasion of privacy if disclosed. b. The policy must clearly detail the types of PII that have been designated as directory information, the parent's or eligible student's right to refuse to let any or all of these types of PII be designated as directory information, and the period of time that the parent or eligible student has to opt out of such a disclosure of directory information. 2. A school and/or LEA must give a public notice to parents of students in attendance and eligible students in attendance prior to disclosing directory information. 3. Subject to a few exceptions, parents or eligible students must not have opted out of the disclosure of directory information.	1. A school and/or LEA must a. Establish criteria in the annual notification of FERPA rights about who is a "school official" and what constitutes a "legitimate educational interest"; b. Determine that the disclosure is to a school official who has a legitimate educational interest in the education records; and c. Use reasonable methods to ensure that school officials obtain access to only those education records in which they have a legitimate educational interest. 2. If outsourcing institutional services or functions to a third party, outside parties may be considered "school officials" if the outside party a. Performs an institutional service or function for which the school would otherwise use employees; b. Is under the direct control of the school with respect to the use and maintenance of education records; and c. Complies with the PII from education records use and redisclosure requirements.	1. The disclosure of PII from student education records must be for, or on behalf of, an educational agency or institution, in order to a. Develop, validate, or administer predictive tests; b. Administer student aid programs; or c. Improve instruction. 2. An educational agency or institution may disclose PII from education records, and a "FERPA-permitted entity" may redisclose PII only if a. The disclosing educational entity enters into a written agreement with the organization; b. The study does not permit identification of individual parents and students by anyone other than representatives of the organization with legitimate interests in the information; and c. The information is destroyed when no longer needed for the study purposes.	1. The disclosure of PII from education records must be to a. Audit or evaluate a Federal- or State-supported education program; or b. Enforce or comply with Federal legal requirements related to the program. 2. The receiving entity must be a State or local educational authority or other FERPA-permitted entity or must be an authorized representative of a State or local educational authority or other FERPA-permitted entity. 3. The party disclosing the PII from education records a. Must enter into a written agreement to designate anyone other than its employee as its authorized representative (each new audit, evaluation, or enforcement effort requires an agreement); and b. Is responsible for using reasonable methods to ensure to the greatest extent practicable that the authorized representative i. Uses the PII only for the authorized purpose; ii. Protects the PII from further unauthorized disclosures or other uses; and iii. Destroys the PII when no longer needed for the authorized purpose and in accordance with any specified time period set forth in a written agreement. 4. State and local educational authorities and other FERPA-permitted entities may redisclose the PII on behalf of the educational agency or institution. In particular, a. The disclosure must meet the requirements of an exception to consent in § 99.31 and either the educational agency or institution or other FERPA-permitted entity has complied with the recordkeeping requirements. 5. Authorized representatives of the FERPA-permitted entities may only redisclose the PII when expressly authorized in the parties' written agreement (assuming that the redisclosure by the authorized representative on behalf of the FERPA-permitted entity would be permissible under FERPA).
Legal references			
34 CFR §§ 99.3, 99.31(a)(11), and 99.37.	34 CFR §§ 99.31(a)(1) and 99.7(a)(3)(iii).	34 CFR § 99.31(a)(6).	34 CFR §§ 99.31(a)(3) and 99.35.
Other notes			
Recordation: FERPA does not require educational agencies and institutions to record disclosures of appropriately designated directory information (§ 99.32(d)(4)).	*Recordation*: FERPA (§ 99.32(d)(2)) does not require educational agencies and institutions to record disclosures of PII from education records to school officials under § 99.31(a)(1).	*Recordation*: FERPA requires educational agencies and institutions to record all disclosures of PII from education records to organizations made under the studies exception (§ 99.32).	*Recordation*: FERPA requires educational agencies and institutions to record all disclosures of PII from education records made under the audit or evaluation exception (§ 99.32). ➢ State and local educational authorities (and other FERPA-permitted entities listed in § 99.31(a)(3)) redisclosing PII on behalf of the educational agency or institution must record disclosures according to the requirements in § 99.32(b)(2).

* *While FERPA does not require that schools implement a directory information policy, if they do so, certain conditions must be met.*

See PTAC website for Additional Resources and Glossary: *http://ptac.ed.gov*

The Family Educational Rights and Privacy Act
Guidance for Reasonable Methods and Written Agreements

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.

Purpose

The audience for this document includes schools, school districts (also referred to as local education agencies [LEAs]), postsecondary institutions, and state educational authorities (such as state education agencies [SEAs]) that may disclose personally identifiable information (PII) from education records. Our intent is to provide these entities with information about requirements and best practices for data disclosures under the studies exception and the audit or evaluation exception.

Background

The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g, is a Federal privacy law administered by the Family Policy Compliance Office (FPCO or Office) in the U.S. Department of Education (Department or we). FERPA and its implementing regulations in 34 CFR part 99 protect the privacy of students' education records and afford parents and eligible students (i.e., students who are 18 years of age or older or attend an institution of postsecondary education) certain rights to inspect and review education records, to seek to amend these records, and to consent to the disclosure of PII from education records.

The general rule under FERPA is that PII from education records cannot be disclosed without written consent. However, FERPA includes several exceptions that permit the disclosure of PII from education records without consent. Two of these exceptions are discussed in this document: the studies exception and the audit or evaluation exception. The two exceptions contain specific, and slightly different, requirements, described more fully in the implementing regulations (34 CFR Part 99).

What is the Studies Exception?
(see 20 U.S.C. §1232g(b)(1)(F) and §99.31(a)(6))

The studies exception allows for the disclosure of PII from education records without consent to organizations conducting studies for, or on behalf of, schools, school districts, or postsecondary institutions. Studies can be for the purpose of developing, validating, or administering predictive tests; administering student aid programs; or improving instruction.

> Example: An SEA may disclose PII from education records without consent to an organization for the purpose of conducting a study that compares program outcomes across school

districts to further assess what programs provide the best instruction and then duplicate those results in other districts.

What is the Audit or Evaluation Exception?

(see 20 U.S.C. 1232g(b)(1)(C), (b)(3), and (b)(5) and §99.31(a)(3) and 99.35)

The audit or evaluation exception allows for the disclosure of PII from education records without consent to authorized representatives of the Comptroller General of the U.S., the Attorney General, the Secretary of Education, and state or local educational authorities (FERPA-permitted entities). Under this exception, PII from education records must be used to audit or evaluate a Federal- or state-supported education program, or to enforce or comply with Federal legal requirements that relate to those education programs (audit, evaluation, or enforcement or compliance activity). The entity disclosing the PII from education records is specifically required to use reasonable methods to ensure to the greatest extent practicable that its designated authorized representative complies with FERPA and its regulations.

> Example: An LEA could designate a university as an authorized representative in order to disclose, without consent, PII from education records on its former students to the university. The university then may disclose, without consent, transcript data on these former students to the LEA to permit the LEA to evaluate how effectively the LEA prepared its students for success in postsecondary education.

How do you define "education program"?

"Education program" is an important term under the audit or evaluation exception because PII from education records can only be disclosed to audit or evaluate a Federal- or state-supported "education program," or to enforce or to comply with Federal legal requirements related to an education program. As specified in the FERPA regulations, §99.3, an education program must be 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. For a definition of "early childhood program" please refer to §99.3 of the FERPA regulations.

Do we need to have a written agreement to disclose PII from education records without consent?

Yes. Both the studies exception and the audit or evaluation exception specifically require that the parties execute a written agreement when disclosing PII from education records without consent. The mandatory elements of that agreement vary slightly between the two exceptions.

Mandatory provisions for written agreements under the studies exception

Written agreements under the studies exception must be in accordance with the requirements in §99.31(a)(6)(iii)(C):

1. Specify the purpose, scope, and duration of the study and the information to be disclosed.
2. Require the organization to use PII from education records only to meet the purpose or purposes of the study as stated in the written agreement.

3. Require the organization to conduct the study in a manner that does not permit the personal identification of parents and students by anyone other than representatives of the organization with legitimate interests. This typically means that the organization should allow internal access to PII from education records only to individuals with a need to know, and that the organization should take steps to maintain the confidentiality of the PII from education records at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques.

4. Require the organization to destroy all PII from education records when the information is no longer needed for the purposes for which the study was conducted, and specify the time period in which the information must be destroyed. You should determine the specific time period for destruction based on the facts and circumstances surrounding the disclosure and study. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit.

Mandatory provisions for written agreements under the audit or evaluation exception

The mandatory provisions for written agreements under the audit or evaluation exception are similar to, but slightly different from, the provisions required for written agreements under the studies exception. Section 99.35(a)(3) specifically requires that the following provisions be included in written agreements under the audit or evaluation exception:

1. Designate the individual or entity as an authorized representative. Your agreement must formally designate the individual or entity as an authorized representative.

2. Specify the PII from education records to be disclosed. Your agreement must identify the information being disclosed.

3. Specify that the purpose for which the PII from education records is being disclosed to the authorized representative is to carry out an audit or evaluation of Federal- or state-supported education programs, or to enforce or to comply with Federal legal requirements that relate to those programs. Your agreement must state specifically that the disclosure of the PII from education records is in furtherance of an audit, evaluation, or enforcement or compliance activity.

4. Describe the activity with sufficient specificity to make clear that it falls within the audit or evaluation exception. This must include a description of how the PII from education records will be used. The agreement must describe in detail the methodology and why disclosure of PII from education records is necessary to accomplish the audit, evaluation, or enforcement or compliance activity.

5. Require the authorized representative to destroy the PII from education records when the information is no longer needed for the purpose specified. Your agreement should be clear about how the PII from education records will be destroyed.

6. Specify the time period in which the PII must be destroyed. You should determine the specific time period for destruction based on the facts and circumstances surrounding the disclosure and activity. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit.

7. Establish policies and procedures, consistent with FERPA and other Federal and state confidentiality and privacy provisions, to protect PII from education records from further disclosure (except back to the disclosing entity) and unauthorized use, including limiting use of PII from education records to only authorized representatives with legitimate interests in an audit, evaluation, or enforcement or compliance activity. The agreement must establish the policies and procedures, consistent with FEPRA and other Federal and state laws, to protect PII from education records from further disclosure or unauthorized use.

Can an entity receiving PII from education records disclose it in a way that allows individual students to be identified?

No. Absent consent from the parent or eligible student, FERPA provides that the PII from education records cannot be published in a way that would allow individual students and their parents to be identified. The organization conducting the study, audit, or evaluation can use PII from education records to conduct the study, audit, or evaluation, but results must be published in a way that protects the privacy and confidentiality of the individuals involved. For example, when publishing tables, cell suppression and other methods of disclosure avoidance can be used so that students cannot be identified through small numbers displayed in table cells. For more information, see Data De-identification: an Overview of Basic Terms and Frequently Asked Questions - Disclosure Avoidance, both available from the Privacy Technical Assistance Center, https://studentprivacy.ed.gov.

Under the audit or evaluation exception, what is your responsibility to use "reasonable methods" to ensure that your authorized representative is FERPAR compliant to the greatest extent practicable?

(See §99.35(a)(2))

When you disclose PII from education records under the audit or evaluation exception, you are required to use "reasonable methods" to ensure to the greatest extent practicable that your authorized representative is FERPA-compliant. This specifically means ensuring that your authorized representative does the following:

1. Uses PII from education records only to carry out an audit or evaluation of Federal- or state-supported education programs, or for the enforcement of or compliance with Federal legal requirements related to these programs. You should make sure that the proposed audit or evaluation is legitimate, and require in your written agreement that your authorized representative use the PII from education records only for that audit, evaluation, or enforcement or compliance activity. You should not disclose all of your PII from education records; rather, you should determine which specific elements your authorized representative needs and disclose only those.

2. Protects the PII from education records from further disclosures or other uses, except as authorized by you in accordance with FERPA. Your agreement must specify that your authorized representative may not further disclose the PII from education records, unless authorized. Approval to use the PII from education records for one audit or evaluation does not confer approval to use it for another.

3. Destroys the PII from education records when no longer needed for the audit, evaluation, or enforcement or compliance activity. Your agreement must specify that your authorized representative is required to destroy the PII from education records when it is no longer needed and specify the time period in which the PII must be destroyed.

Are there best practices that support reasonable methods?

Yes. While it is vital for organizations to comply with FERPA and its regulations, FERPA represents the floor for protecting privacy, not the ceiling. Accordingly, the Department specifies best practices, in which we describe actions we recommend you take to ensure that your authorized representative is protecting privacy to the greatest extent possible. Best practices are broader than FERPA requirements and describe recommended actions you should take to ensure that your authorized representative is FERPA-compliant to the greatest extent practicable.

These best practices may apply to data sharing under both the audit and evaluation exception and the studies exception. Please keep in mind that not all of the following best practices are appropriate in every instance, and this list does not include every possible protection. Before disclosing PII from education records under one of these exceptions, you should examine the following list and tailor your practices as necessary and appropriate.

- *Convey the limitations on the data.* You should take steps to ensure your authorized representative knows the limitations on the use of the data.
- *Obtain assurances against redisclosure.* You should obtain assurances from your authorized representative that the data will not be redisclosed without permission, including such assurances that your authorized representative will provide you (the disclosing entity) the right to review any data prior to publication and to verify proper disclosure avoidance techniques have been used.
- *Be clear about destruction.* You should set clear expectations so your authorized representative knows what process needs to be followed for the proper destruction of PII from education records.
- *Maintain a right to audit.* You should maintain the right to conduct audits or other monitoring activities of your authorized representative's policies, procedures, and systems.
- *Verify the existence of disciplinary policies to protect data.* You may want to verify that your authorized representative has appropriate disciplinary policies for employees that violate FERPA. This can include termination in appropriate instances.
- *Verify the existence of a sound data security plan.* Before disclosing PII from education records, you may wish to verify that your authorized representative has a sound data security program, one that protects both data at rest and data in transmission. You have a responsibility to determine if your authorized representative's data security plan is adequate to prevent FERPA violations. The steps that you may need to take in order to verify a sound data security program are likely to vary with each situation. In some cases, it may suffice to add language to the written agreement that states what data security provisions are required. In other cases, it may be more prudent for you to take a hands-on approach and complete a physical inspection. Additionally, your written agreements could specify required data security elements, including requirements related to encryption, where the data can be hosted, transmission methodologies, and provisions to prevent unauthorized access.
- *Verify the existence of a data stewardship program.* You may want to examine your authorized representative's data stewardship program. Data stewardship should involve internal control procedures that protect PII from education records and include all aspects of data collection, from

planning to maintenance to use and dissemination. The Department believes that a good data stewardship plan would have support and participation from across the organization, including the head of the organization; management; legal counsel; and data administrators, providers, and users. The plan should detail the organization's policies and procedures to protect privacy and data security, including the ongoing management of data collection, processing, storage, maintenance, use, and destruction. The plan could also include designating an individual to oversee the privacy and security of the PII from the education records it maintains. For more information, see the technical brief Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records.

- *Disclose only PII from education records that is needed.* When you consider disclosing PII from education records to an authorized representative for an audit, evaluation, or enforcement or compliance activity, you may want to explore which specific data elements are necessary for that activity and provide only those elements. You should take care to ensure that you are not disclosing more PII from education records than needed for the stated activity and purpose. You should also explore whether PII from education records is actually required, or whether de-identified data would suffice.

- *Know to whom you are disclosing data.* You may want to require your authorized representative to conduct background investigations of employees who will have access to PII from education records, or you may want to conduct these investigations yourself. Additionally, you may want to require your authorized representative to disclose past FERPA or data management violations. If you discover past violations, you would want to explore the circumstances behind the violation, and discover all information that would allow you to make an informed judgment on whether the individual or entity is likely to be a responsible data steward. This may include discovering whether the violation was covered up, if it was voluntarily reported to affected students or FPCO, and whether appropriate breach response procedures were followed.

- *Verify training.* You may want to verify that your authorized representative has a training program to teach its employees about FERPA and how to protect PII from education records, or you may want to train your authorized representatives yourself.

Are there best practices for written agreements?

You should consider the following items for inclusion in your written agreements for work under both the audit or evaluation exception and the studies exception. We note that this list may not cover everything you want in your agreement; you should look to the facts and circumstances surrounding the disclosure agreement and include all terms necessary to be clear about roles, responsibilities, and expectations for safeguarding PII from education records.

- *Bind individuals to the agreement.* It can be important to bind not just the entity to whom you are disclosing PII from education records, but also the individuals who will be accessing that data. There are several ways to accomplish this result. One way is to identify the individuals in the agreement itself, and have them execute the agreement in their individual capacity as well as having a representative execute the agreement for the entity. Alternatively, your agreement can require individuals accessing the PII from education records to execute affidavits of nondisclosure or other

documentation indicating their individual agreement to handle the PII from education records properly.

- *Agree on limitations on use of the PII from education records.* Your agreement should be clear about limitations on the use of the PII from education records, meaning that it can only be used for the activities described in the agreement. Your agreement may also address methodological limitations: for example, identifying to which datasets, if any, the PII from education records may be linked.

- *Agree to not redisclose.* The most basic provision of the agreement is to make clear that the PII from education records is confidential and must not be redisclosed through direct data disclosures or publishing results that allow individuals to be directly or indirectly identified. FERPA-permitted entities may wish to require that specified disclosure avoidance methodologies be applied, or may wish to review all results prior to publication, or both.

- *Specify points of contact/data custodians.* Your written agreements should specify points of contact and data custodians (the individuals directly responsible for managing the data in question).

- *Mention Institutional Review Board (IRB) review and approval.* While FERPA does not mention IRBs, research proposals involving human subjects may have to be reviewed and approved by IRBs, if required under protection of human subject regulations of the Department and other Federal agencies. If IRB review and approval is required or expected, this may be noted in the written agreement.

- *State ownership of PII from education records.* You may wish for your agreement to be clear that, in disclosing PII from education records to an entity, you are in no way assigning ownership of the PII or records to that entity, and that it may only be redisclosed with your permission or otherwise in compliance with FERPA and its regulations.

- *Identify penalties.* Your agreement could include penalties under state contract law such as liquidated damages, data bans of varying length, and any other penalties the parties to the agreement deem appropriate. You may want your agreement to create third-party beneficiary rights, e.g., allowing parties injured by a data breach to sue for damages. While FERPA itself has little flexibility for sanctions, you can include a wide range of appropriate sanctions in your written agreements.

- *Set terms for data destruction.* As discussed previously, written agreements for both studies and audits and evaluations are required to contain provisions dealing with the destruction of PII from education records when those records are no longer needed. The agreement could include a method for documenting the destruction, such as the use of notarized statements.

- *Include funding terms.* If the agreement involves cost reimbursement, these details could be specified.

- *Maintain right to audit.* You may want to include the right to conduct audits or otherwise monitor the entity to which you are disclosing PII from education records to periodically affirm that the entity has appropriate policies and procedures in place to protect the PII from education records.

- *Identify and comply with all legal requirements.* It is important to remember that FERPA may not be the only law that governs your agreement. The agreement could broadly require compliance with all applicable Federal, state, and local laws and regulations, and identify the legal authority (whether express or implied) that permits the audit, evaluation, or enforcement or compliance activity.

- *Have plans to handle a data breach.* While no one anticipates a data breach, data loss may occur. You may wish to include specific procedures in your written agreements detailing the parties' expectations in the event that PII from education records is lost, including specifying the parties' responsibilities with regard to breach response and notification and financial responsibility.

- *Review and approve reported results.* If applicable, the written agreement could specify the parties' agreements with respect to publication of results. For example, you may wish to review and approve reports prior to publication to make sure that they reflect the original intent of the agreement.

- *Define terms for conflict resolution.* The agreement could specify procedures for how disputes between the parties would be resolved.

- *Specify modification and termination procedures.* The agreement could specify how it can be modified or terminated. You may wish to provide specific provisions for termination based on improper handling of PII from education records.

What do I do if the terms of the written agreement are violated?

If the entity to which you have disclosed PII from education records without consent (whether under the studies exception or the audit and evaluation exception) violates the terms of the written agreement, you should evaluate your options under the penalty and termination provisions of the agreement. You may want to stop disclosing PII from education records to that organization, or pursue legal redress. If you have reason to believe that the entity has violated FERPA, you should contact FPCO.

How should the public be informed?

It is a best practice to keep the public informed when you disclose PII from education records.

- *Inform the public about written agreements.* Transparency is a best practice. You might want to post your data sharing agreements on your website, or provide some equivalent method to let interested parties know what data you are disclosing, the reasons the data are being disclosed, and how the data are being protected. While the Department generally recommends public posting of written agreements, parties are encouraged to review their contractual data security provisions carefully and redact, prior to publication, any provisions that may aid those seeking unauthorized access to systems. In certain instances a separate confidential IT Security Plan may be appropriate. For more information on data security best practices, see the Privacy Technical Assistance Center (PTAC) website: https://studentprivacy.ed.gov

What if I have more questions?

If you would like more information about best practices to protect PII from education records, go to https://studentprivacy.ed.gov, contact the PTAC Help Desk at PrivacyTA@ed.gov , or call 855-249-3072.

If you are a parent, eligible student, school, LEA, or SEA and would like more information on FERPA, please visit https://studentprivacy.ed.gov or call FPCO at 1-800-872-5327.