Protecting Student Privacy while Creating and Using Integrated Data Systems

Requirements and Best Practices

December 3, 2014

AISP Developing Sites Conference

University of Pennsylvania

Michael Hawes
Statistical Privacy Advisor
U.S. Department of Education

Overview

- FERPA Basics
- Applying FERPA in the IDS Context
- Best Practice Recommendations
- Available Resources
- Q & A

The U.S. Department of Education's Role in Protecting Student Privacy

- Administering and enforcing federal laws governing the privacy of student information
  - Family Educational Rights and Privacy Act (FERPA)
  - Protection of Pupil Rights Amendment (PPRA)
- Raising awareness of privacy challenges
- Providing technical assstance to schools, districts, and states
- Promoting privacy & security best practices

FERPA Basics

A brief summary of key concepts and definitions

Family Educational Rights and Privacy Act (FERPA)

- Gives parents (and eligible students) the right to access and seek to amend their children's education records
- Protects personally identifiable information (PII) from education records from unauthorized disclosure
- Requirement for written consent before sharing PII – unless an exception applies

(20 U.S.C. §1232g & 34 CFR Part 99)

Personally Identifiable Information (PII) under FERPA

- Direct Identifiers
  - Name
  - Name of parents or other family members
  - Address
  - Identifying Number (e.g., SSN, Student ID#)
  - etc.

- Indirect Identifiers (e.g., date or place of birth)

- *"Other information that, alone or in combination, 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." (§ 99.3)*

Education Records under FERPA

"Education Records" are records:

- Directly related to the student; and
- Maintained by (or on behalf of) an educational agency or institution.

But wait! There are exceptions!

FERPA includes a number of exceptions that permit disclosing PII for certain purposes without parental consent:

- "Directory Information"
- School Officials
- "Studies"
- "Audits and Evaluations"
- Health and Safety emergencies

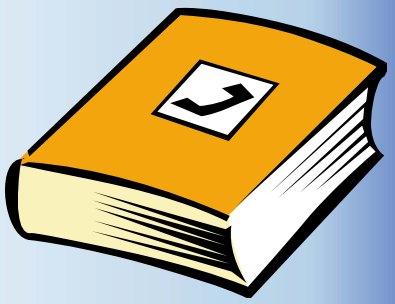
among others.

See §99.31 for information on other FERPA exceptions and their requirements.


“Research Exception”

Directory Information Exception

- Students don't attend school anonymously.
- Allows schools to release certain information without consent. A few examples:
  - name, address, telephone listing, electronic mail address;
  - date and place of birth;
  - photographs;
  - weight and height of athletes;
  - degrees & awards received, etc.



Directory Information Exception

- Schools/Districts must designate the data elements they consider to be Directory Information.
- Common uses:
  - Yearbooks
  - Concert programs
  - Telephone directories

Parents have a right to opt-out of disclosures under the Directory Information exception!

School Official Exception

- Schools or LEAs can use the School Official exception to disclose education records to a third party if the third party:
  - Performs a service/function for the school/district for which it would otherwise use its own employees
  - Is under the direct control of the school/district with regard to the use/maintenance of the education records
  - Uses education data in a manner consistent with the definition of the "school official with a legitimate educational interest," specified in the school/LEA's annual notification of rights under FERPA

Studies Exception

- "For or on behalf of" schools, school districts, or postsecondary institutions
- Studies must be for the purpose of
  - Developing, validating, or administering predictive tests; or
  - Administering student aid programs; or
  - Improving instruction
- Written agreement requirement

Written Agreements—Studies Exception

- Written agreements must
  - Specify the purpose, scope, and duration of the study and the information to be disclosed, and
  - Require the organization to
    - use PII only to meet the purpose(s) of the study
    - limit access to PII to those with legitimate interests
    - destroy PII upon completion of the study and specify the time period in which the information must be destroyed

Audit/Evaluation Exception

Allows PII from education records to be shared without consent with

- "Authorized representatives" of
- "FERPA-permitted entities":
  - Comptroller General of U.S.,
  - U.S. Attorney General,
  - U.S. Secretary of Education, and
  - State or Local Educational Authorities

34 CFR Section 99.31(a)(3)

Audit/Evaluation

- Data can only be shared in order to
  - Audit or evaluate a Federal- or State-supported education program, or
  - Enforce or comply with Federal legal requirements that relate to those education programs
- "Education program" – broad, but not limitless
  - Any program principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, and any program that is administered by an educational agency or institution (FERPA regulations § 99.3)

Written Agreements—Audit/Evaluation Exception

- Written agreements must
  - Designate an authorized representative
  - Specify what PII will be disclosed and for what purpose
  - Describe the activity to make clear that it falls within the audit/evaluation exception
  - Require an authorized representative to destroy PII upon completion of the study and specify the time period in which the information must be destroyed
  - Establish policies and procedures, consistent with FERPA and other Federal and State confidentiality and privacy laws, to protect PII from further disclosure and unauthorized use

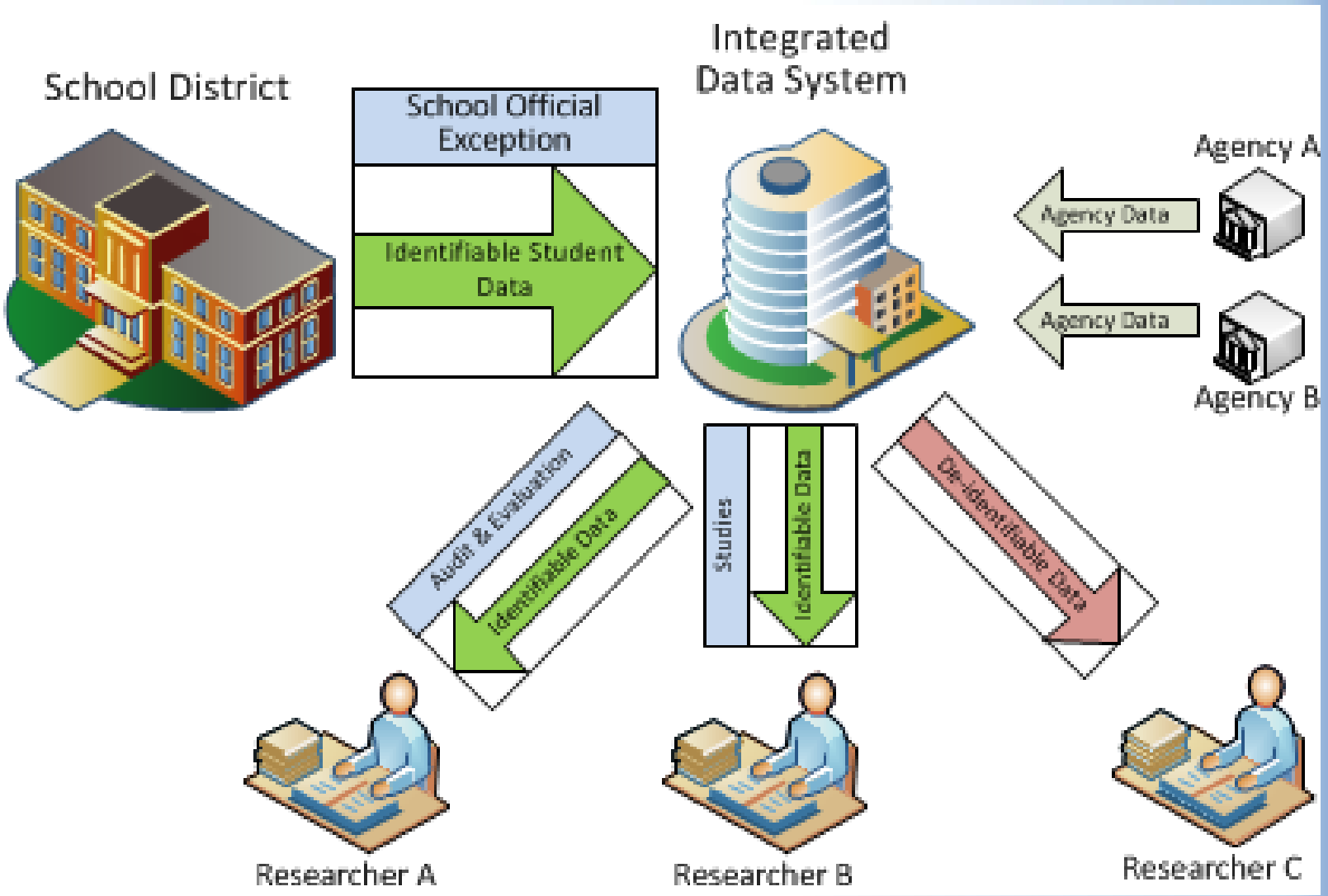
FERPA and Integrated Data Systems

How FERPA applies to the creation and use of IDS

Which Exception to Use?

- From the IDS perspective, there are pros and cons to using each of the FERPA exceptions
- In most cases, no single exception will permit both the creation and use of an IDS (especially if external researchers are involved)
- A better (and more easily managed) approach is to use a multi-stage process

How it works


School District
School Official Exception
Identifiable Student Data
Integrated Data System
Agency A
Agency Data
Agency Data
Agency B
Audit & Evaluation
Identifiable Data
Studies
Identifiable Data
De-identifiable Data
Researcher A
Researcher B
Researcher C

Stage 1: Creating the IDS

To create an IDS, schools and districts should* use FERPA's School Official exception.

Make sure the requirements of the School Official exception are met, including:

- Annual FERPA Notice Requirements:
  - Establish linkage and research as a legitimate educational purpose
  - Ensure IDS staff are covered by the definition of "school official"
- "Direct Control" Requirement
- Authorize IDS to approve "Studies" and/or to designate "Authorized Representatives" (optional)

**In some circumstances, an IDS may be created under FERPA's Audit and Evaluation exception, but the logistics (especially regarding recordation and redisclosure) can get much more complicated.*

Stage 2: Using Education Data in an IDS

Once the IDS is created and operational, there are a number of pathways for permitting research using the linked data, including:

- Studies Exception
- Audit and Evaluation Exception
- Deidentified Data

Stage 2: Studies Exception

Under the Studies exception:

- The research must be:
  - "for, or on behalf of, the school or district," and
  - intended to "improve instruction" (or one of the other allowable purposes); and
- There must be a written agreement* between the researcher and either the school/district, or the IDS (acting as a School Official)

*See http://ptac.ed.gov for guidance on written agreements under FERPA

Stage 2: Audit and Evaluation Exception

Under the Audit and Evaluation exception:

- The research must be to audit or evalute a federal or state supported education program
- There must be a written agreement* between the researcher and either the district, or the IDS (acting as a School Official) designating the researcher as the district's "authorized representative"

*See http://ptac.ed.gov for guidance on written agreements under FERPA

Stage 2: Deidentified Data

If neither the Studies nor the Audit and Evaluation exceptions can apply, research may still be performed using linked IDS data, if the IDS staff (acting in their School Official capacity):

- deidentify the data by removing all direct and indirect identifiers;
- as needed, perform statistical methods to reduce the risk of reidentification, including:
  - aggregation,
  - suppression,
  - blurring, or
  - perturbation; and
- perform a disclosure avoidance analysis on the resulting file to determine that it meets FERPA's standards for reidentification.

Best Practice Recommendations

Transparency Best Practices

- Be open about what data you are collecting and linking
- Explain (in layman's terms) what research and analysis you are doing (and why!)
- Publish (and advertise) the strength of your data governance and information security practices
- Use a multi-layered communication strategy
- Value! Value! Value! (Explain what's in it for the parents/children)

Take Home Points:

- FERPA is not the insurmountable obstacle to data access/use that many think it is.

  But, there are important requirements and data use restrictions that you must follow.
- Aggregate data are often still FERPA-protected PII.
- Just because something is legal, doesn't mean it's a good idea!
- Be open about what you're doing
- Highlight your successes

Resources

Privacy Technical Assistance Center (PTAC)

Website: http://ptac.ed.gov

Email: PrivacyTA@ed.gov

- FAQs
- Issue Briefs
- Case Studies
- Checklists
- Site Visits
- Help Desk

Questions and Discussion

Michael Hawes
Statistical Privacy Advisor
U.S. Department of Education
Michael.Hawes@ed.gov
(202) 453-7017