Protecting Student Privacy

FERPA Overview and Best Practice Recommendations from the U.S. Department of Education

August 19, 2014

CSDE Data and Performance Summit

Cromwell, CT

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

Overview

- The U.S. Department of Education's role in protecting student privacy
- Family Educational Rights and Privacy Act (FERPA)
- Rise in public discourse on student privacy
- Highlights from recent ED guidance

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 assistance to schools, districts, and states
- Promoting privacy & security best practices

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*

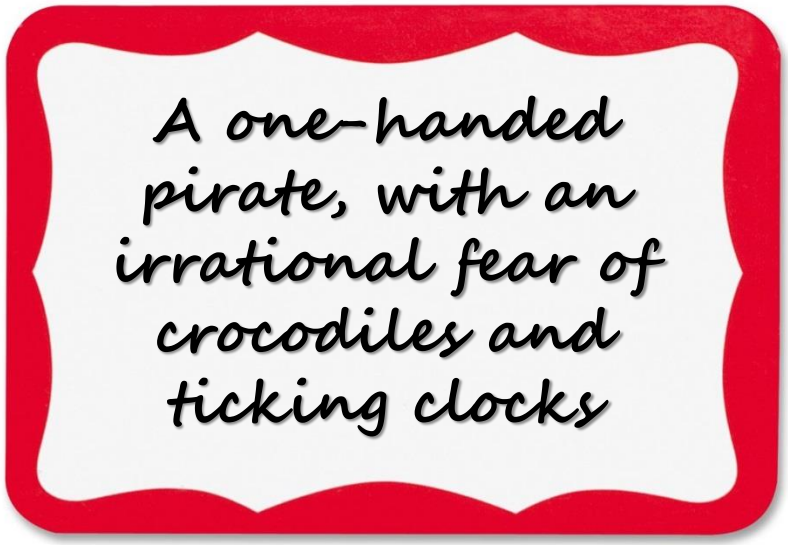
"Education Record" = Information directly related to a student, that is maintained by (or on behalf of) a school or school district

PII is:

Personal Information

PII is:

Personally Identifiable Information



Personally Identifiable Information (PII) under FERPA

- Name
- Name of parents or other family members
- Address
- Personal identifier (e.g., SSN, Student ID#)
- Other 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)*

But Wait! There are Exceptions!

Commonly used exceptions to FERPA's written consent requirement:

- Directory information exception
- School official exception
- Health and safety emergencies exception
- Studies exception
- Audit and evaluation exception
- and more…

Recent Developments

- inBloom
- State Legislation – the latest estimate is that there were 110 bills introduced in 36 states this year (26 passed) that deal with student privacy. The bills differ, but generally:
  - Forbid collection of certain data
  - Forbid districts from sharing certain data with the state
  - Appoint a CPO
  - Include provisions relating to:
    - Data governance
    - Transparency
    - Cloud computing

A New Concern: Marketing Student Data

- Center for Law and Information Policy report on district contracting for online services

("Fordham Study")

The Challenge of Online Educational Services

- Schools and districts are increasingly contracting out school functions
- We have new types of data, and much more of it!
- Many online services do not utilize the traditional 2-party written contractual business model
- Increasing concern about the commercialization of personal information and behavioral marketing
- We need to use that data effectively and appropriately, and still protect students' privacy

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
  - Does not re-disclose or use education data for unauthorized purposes

Are providers limited in what they can do with the student information they collect or receive?

If PII is disclosed under the Directory Information exception:

- No limitations

If PII is disclosed under the School Official exception:

- PII from education records may only be used for the specific purpose for which it was disclosed
- TPPs may not sell or share the PII, or use it for any other purpose except as directed by the school/district and as permitted by FERPA

When personal information is collected from a student, the PPRA may also apply!

- *PPRA places some limitations on the use of personal information collected from students for marketing*

Are providers limited in what they can do with the student information they collect or receive?

Remember, schools and districts have an important role in protecting student privacy.

Additional limitations and restrictions (beyond what FERPA, PPRA, and other laws require) may be written into the agreement between the school/district and the provider!

Be careful when using "free" educational services

Remember the FERPA's requirements for schools and districts disclosing PII under the school official exception.

- Direct control
- Consistency with annual FERPA notice provisions
- Authorized use
- limits on re-disclosure

These services may also introduce security vulnerabilities into your school networks

It is a best practice to establish district/school level policies governing use of free services, and to train teachers and staff accordingly.

Transparency Best Practices

- Let parents know what information you're collecting, and why you're collecting it
- Inform parents about your data governance and information security practices
- Use a multi-layered communication strategy
- Be open about who you share data with, and why. (Post your data sharing contracts and MOUs)
- Value! Value! Value! (Explain what's in it for the parents/children)

Remember:

- In the absence of information, people tend to assume the worst
- Just because something is legal, doesn't mean it's a good idea!
- Be open about what you're doing
- Highlight your successes

PTAC Resources

- PTAC breakout session **"FERPA 101: Protecting Student Data in the 21st Century"** [Ballroom A/B/C/D]
- PTAC Toolkit: http://ptac.ed.gov/toolkit
  - Issue Briefs
  - Checklists
  - FAQs
  - Case Studies
  - Webinars
  - Etc.

PTAC Contact Information

Privacy Technical Assistance Center

(855) 249-3072

http://ptac.ed.gov

PrivacyTA@ed.gov