An Update on FERPA and Student Privacy

September 30, 2014
Legal Issues in Higher Education Conference

Kathleen M. Styles
Chief Privacy Officer
U.S. Department of Education

Presentation Agenda

- A few FERPA basics
- Hot Topics
- Issues in Higher Education
- Final thoughts

Privacy Challenges on Campus

Let's set the stage:

- Many colleges are data factories.
- Data management in many colleges is highly siloed.
- Big data has found a home in higher ed.
- Most campuses have data that is protected by a variety of federal and state statutes.
- Students, by their very nature, can be challenging data subjects.
FERPA – Everyone’s Favorite Statute

FERPA – Access & Consent

- 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
- General requirement to obtain written consent before sharing PII

But Wait! There are Exceptions!

- FERPA has a number of exceptions, including:
  - Directory information
  - School officials
  - Audit and evaluation
  - Studies
- There are many other FERPA exceptions
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.

School Official Exception

- IHEs can use the School Official exception to disclose education records to a third party provider if the provider:
  - Performs a service/function for the IHE for which it would otherwise use its own employees
  - Is under the direct control of the IHE 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 IHE’s annual notification of rights under FERPA
  - Does not re-disclose or use education data for unauthorized purposes

Our Favorite FERPA Quote

“You know how sometimes FERPA can tie your brain in a knot trying to think through it all?”

Received in an email to PTAC
**What Do You Think?**

Which of the following do you think is the most common question that we receive in the Family Policy Compliance Office related to higher education:

1. MOOCs – does FERPA apply to MOOCs?
2. Parents – do they have a right to see grades for their children in college?
3. Data sharing – can/should IHEs share data with state boards of education to allow the production of “High School Feedback Reports?”
4. Data breaches – does the school have to notify the students whose information was breached?

---

**FERPA Administration**

- FPCO: Family Policy Compliance Office
- **New**: PTAC, the Privacy Technical Assistance Center
- **New**: Executive level Chief Privacy Officer
- Compliance – 400-500 formal complaints/year
- Technical assistance – 12-15 thousand phone calls/year, plus about 2 thousand emails/year
- Remedies and enforcement

---

**Recent Developments**

- State longitudinal data systems and increased data sharing for accountability and evaluation
- Lots of media attention, some of it factual
- A new concern: marketing of student information
- Our “Epic FOIA”
Legislative Update

- Lots of calls to “update” FERPA
- “Protecting Student Privacy Act of 2014”
  - Portions would apply to higher ed, as well as K-12
  - Increased requirements for data security
  - Requirement to destroy shared data
  - Other provisions
- In general, however, legislative action has been in the state legislatures (39 states, 110 different bills) and has revolved around K-12 privacy issues.

Legislative Update cont.

The state bills differ, but common provisions include:
- Forbidding the collection of certain data (biometric data, e.g.)
- Forbidding districts from sharing certain data with the state
- Appointing a CPO
- Requiring actions relating to:
  - Data governance
  - Transparency
  - Cloud computing

A New Concern: Marketing Student Data

- Center for Law and Information Policy
- Common Sense Media
- Senator Markey
The Challenge of Online Educational Services

- Institutions are increasingly contracting out school functions
- New types of data, and much more of it
- Many online services do not utilize the traditional two-party written contractual business model
- Increasing concern about the commercialization of personal information and behavioral marketing
- We need to use data effectively and appropriately and still protect students’ privacy

ED Guidance for Online Educational Services

We have recently released guidance about online educational services
- Computer software, mobile applications (apps), or web-based tools
- Provided by a third-party to an educational institution
- Accessed via the Internet by students and/or parents
- Used as part of a school activity

“We must provide our schools, teachers and students cutting-edge learning tools. And we must protect our children’s privacy. We can and must accomplish both goals...

Privacy rules may well be the seatbelts of this generation. I'd like to see vigorous self-policing by the commercial players. Frankly, it's in their interest to do so.”

U.S. Secretary of Education Arne Duncan
February 24, 2014
“Big Data: Seizing Opportunities, Preserving Values”

“The federal government should ensure that data collected in schools is used for educational purposes and continue to support investment and innovation…it should explore how to modernize the privacy regulatory framework under FERPA and COPPA….”

President’s Council of Advisors on Science and Technology
May, 2014

http://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf

“Big Data and Privacy: A Technological Perspective

“In some fantasy world, users actually read [privacy] notices, understand their legal implications (consulting their attorneys if necessary), negotiate with other providers of similar services to get better privacy treatment, and only then click to indicate their consent. Reality is different.”

President’s Council of Advisors on Science and Technology
May, 2014

http://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf

Big Data on Campus

- Where will you find big data on campuses?
  - Mobile Devices
  - University Hospitals
  - Research
  - Think creatively – badging information?
- Using de-identified data is not a panacea
- What is the role of your IRB and what is the role of consent?
Reverse Transfer

- Sometimes students transfer from a community college to a 4-year college or university without receiving their associate’s degree.
- Some postsecondary officials have instituted policies to help students obtain their associate’s degree from their former community college, using the credits earned while attending their 4-year institution.

FERPA and Reverse Transfer

The answers get highly technical. Consider:
1. Disclosure to perform a degree audit
2. Disclosure to award the degree
3. Opt out/opt in for award of the degree

Oklahoma has been using a somewhat unique model.

Student Success Systems

- Many schools are now using student information to provide better services to students, and to improve graduation rates.
- Think about FERPA’s “School Official” exception when evaluating these proposals, but also think about Fair Information Practice Principles.
- Consider the potential that Big Data can be used for discrimination or to limit choice. Example: using student information to disallow certain majors.
Data Breaches

- We do not have good data about data breaches in IHEs, and by any measure this is a huge problem.
- Reporting data breaches to ED?
- Remember, the Gramm-Leach-Bliley Act (GLBA):
  - Administered by the Federal Trade Commission
  - Protects consumer information held by "financial institutions"
  - Yes, IHEs are "financial institutions"

GLBA Safeguards Rule Checklist

Written security policy should contain:
- Administrative requirements
- Technical requirements
- Physical measures
- Documentation needs to be reviewed regularly and after a data security incident
- Regular training on policies and other details are required and need to be implemented
- Internal/external resources should be engaged to verify that the security program is effective
- Policy rules need to be enforced consistently

Challenges of Maintaining Privacy in Higher Ed

- Stovepipe administration – Registrars don’t talk to CIOs, who don’t talk to Attorneys
- Data Security – Many IHEs have a poor understanding of the data they hold and how it is protected
- Big data and new technologies: New types of data and more of it
Massive Open On-line Courses (MOOCs)

- MOOCs are only covered by FERPA if they receive federal funds.
- If they are free, and no federal financial aid is involved, then MOOCs are not covered by FERPA.

Campus Emergencies

We can’t forget the incidents in Tucson and on the Virginia Tech campus.
- FERPA can allow disclosure without consent if necessary to protect the health or safety of a student or other individuals.
- There must be an actual, impending, or imminent emergency. This is intended to be a flexible standard that gives deference to school officials.

Concluding Thoughts

- Institutions need to have an incident response plan.
- Privacy trainings for faculty/staff.
- Know and understand:
  - What data is being collected,
  - Who is collecting it,
  - How it’s being collected,
  - Why it’s being collected, and
  - What is happening to that data.
- Be transparent
  - Be proactive about making data and privacy practices publicly available.
Additional Resources

For additional information on these topics and best practice recommendations please visit our websites

- Family Policy Compliance Office (FPCO):
  http://familypolicy.ed.gov
  • Provides detailed guidance on legal requirements under FERPA and PPRA

- Privacy Technical Assistance Center (PTAC):
  http://ptac.ed.gov
  • Provides guidance documents, trainings, checklists, frequently asked questions, and other resources relating to best practices for data privacy and security

Questions?

This is the most important part – I’d like to hear from you on:

- What challenges are you facing?
- What more can we do to help you?