



Data Use in Higher Education: The Privacy Connection

**July 7, 2015
SHEEO Annual Meeting**

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



Presentation Agenda

- Data use in higher ed – 30,000 foot view
- As always: challenges and opportunities
- Hot topics
- Final thoughts



Where do you find data on campus?

Answer: Everywhere!

- Traditional education data – grades, etc.
- Swipe cards
- IP address logs, campus wi-fi location data
- Discipline records
- Campus provided email and digital storage
- Snaps, vines, tweets, posts, yaks
- Medical information
- Research universities have research data



What is the data being used for?

Think beyond traditional school functions to include

- Accountability
- Civil rights
- Student success systems
- Improving safety

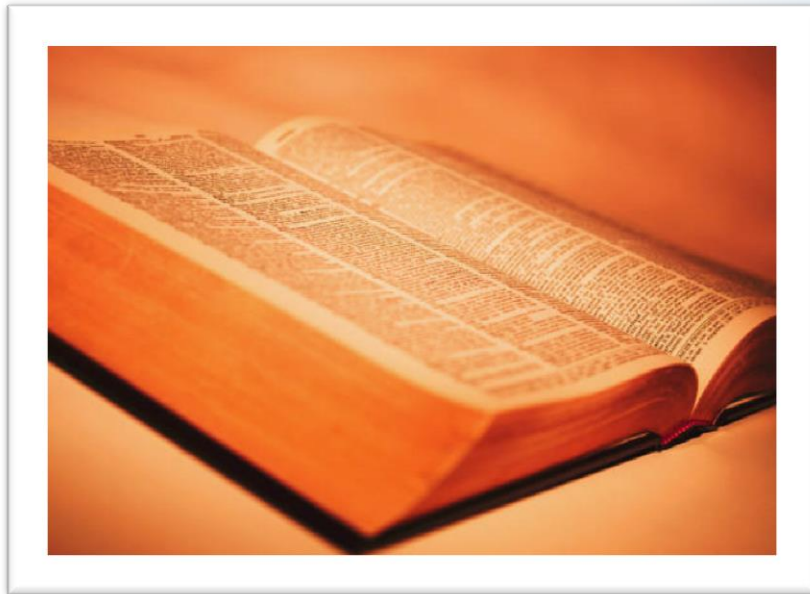


FERPA Administration

- Processing complaints:
 - FPCO, the Family Policy Compliance Office
 - 400 – 500 per year, with the number rising
- Help and Technical Assistance:
 - PTAC, the Privacy Technical Assistance Center
 - 12,000 – 15,000 phone calls/year
 - 2,000 emails per year from school officials
- Policy Development
 - LOTS of new policy documents but still
 - Many unanswered questions
 - The priority list



FERPA: Ripe for Change?





Challenges of Maintaining Privacy in Higher Ed



- “Silos of Excellence” – Registrars don’t talk to CIOs, who don’t talk to Attorneys, who don’t talk to
- 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



Challenges, cont.

- Confusing mishmash of federal and state privacy statutes
- Students, by their very nature, can be challenging data subjects
- Lack of agreement on the role of the IRB for data use decisions





Lots of Very Public Interest

“... data collected on students in the classroom should only be used for educational purposes — to teach our children, not to market to our children. We want to prevent companies from selling student data to third parties for purposes other than education. We want to prevent any kind of profiling that puts certain students at a disadvantage as they go through school.”





Recent Developments

- Increased data sharing for accountability and evaluation
- Lots of media attention, some of it factual
- Lots of political interest
- A new concern: marketing of student information
- Many, many, many new state student privacy statutes



Hot Topics

- Student success systems
- Reverse transfer
- Treatment records
- Data security
- Campus emergencies



Student Success Systems

- Many schools are now using student information to provide better services to students, and to improve graduation rates.
- Consider FERPA's "School Official" exception when evaluating these proposals – but don't stop there!
- Don't forget Fair Information Practice Principles, and don't forget basic ethics.
- "With great data use comes great responsibility."



Reverse Transfer



- Sometimes students transfer from a community college to a 4-year college or university without receiving their associate's degree.
- Some IHEs have instituted processes to help students obtain their associate's degree from their former community college(s), using the credits earned while attending other institutions.

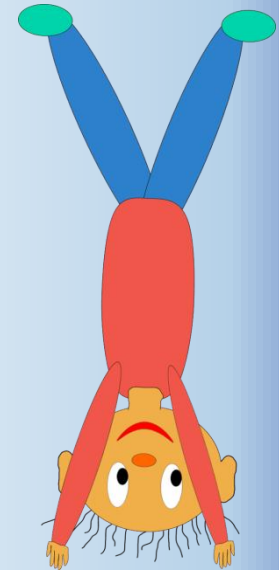


FERPA and Reverse Transfer

Reverse transfer involves disclosures under FERPA:

1. Disclosure to form your universe of eligibles
2. Disclosure to degree granting institution
3. Disclosure to award the degree

Does FERPA allow data sharing for Reverse Transfer? Yes, but there are a number of routes and it's tricky. Call PTAC if you need help.





Treatment Records

“We are concerned about the possibility that FERPA may offer fewer confidentiality protections than the HIPAA Privacy Rule in the limited circumstances where institutions choose to share treatment records with their attorneys in conjunction with litigation between the student and the institution.”

Stay tuned.
More to come.



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”



Campus Emergencies

We can't forget the incidents in Tucson and on the Virginia Tech campus.

- 2011 Guidance: "Addressing Emergencies on Campus"
<http://www2.ed.gov/policy/gen/guid/fpco/pdf/emergency-guidance.pdf>
- 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
- Governance: You should 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 it
- Be transparent
- Legal compliance isn't enough – do the right thing



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