Family Educational Rights and Privacy Act
(FERPA)

An Overview

Office of the Registrar

408 N. Union St.

registrar@indiana.edu

(812) 855-0121

INDIANA UNIVERSITY
BLOOMINGTON

Family Educational Rights and Privacy Act of 1974

- **FERPA** is a federal law "designed to
    1) Protect the privacy of education records;
    2) Establish the right of students to inspect and review their education records, and;
    3) Provide guidelines for the correction of inaccurate and misleading data through informal and formal hearings."

- FERPA is enforced by the Family Policy Compliance Office, U.S. Department of Education, Washington, D.C.

Key Concepts

- *Annual Notification of Student Rights under FERPA*

- *Education record*

- Public vs. private information

- School Official and Legitimate Need

- Requirements for disclosure of student education record

- Exceptions to those requirements as described in the Release of Student Information Policy

INDIANA UNIVERSITY
BLOOMINGTON

Annual Notification
http://registrar.indiana.edu/ferpa.shtml

The Office of the Registrar provides the *Annual Notification of Student Rights under FERPA* to students to inform them of their right to:

- Inspect and review their education records (within 45 days of a request);
- Request an amendment to their education records;
- Request a hearing if the request for an amendment is unsatisfactory;
- Request that the institution not disclose their directory information;
- Informs students how their record will be handled - who will have access and why they will be given access
- File a complaint with the U.S. Department of Education.

Education Records

Education records are directly related to a student and **maintained** by an institution or its agent for all enrolled students, including those also enrolled in **high school**.

Education records include:
- Graded papers
- Exams
- Transcripts
- Class list on your desktop
- Notes from a conversation with a student
- Computer screen displaying student information
- Email containing information about a student

Education records *do not* include:
- Sole possession (lap drawer) records
- Peer graded papers
- Online forums (e.g., Oncourse chats)
- Law enforcement unit records
- Employment records (unless employment is based on student status)
- Medical records
- Alumni records

Public vs. Private Information

- Directory/public information: information contained in the record which would not generally be considered harmful or an invasion of privacy if disclosed

    At IU, this includes name, e-mail address, major, dates of attendance, admission or enrollment status, campus, school, class standing, degrees and awards, activities, sports, and athletic information

- Personally identifiable/private information: would generally be considered more sensitive or an invasion of privacy if disclosed

    At IU, this includes University ID number, Social Security number, grades, hours completed, GPA, **current class schedule**, parent name and address, race, gender, country of citizenship, and date of birth.

School Officials and Legitimate Need

School official

- A person employed by the university in an administrative, supervisory, academic, research, or support position (including law enforcement personnel and health staff);

- A person or company with whom the university has contracted (attorney, auditor, collection agent);

- A person serving on the Board of Trustees;

- A student serving on an official committee (disciplinary, residency or grievance committees) or assisting a school official in completing his or her tasks.

Legitimate need

- Need the information in order to conduct the university business you were asked to perform

Exceptions: What the Institution *May* Honor

- Legitimate educational interest/need to know
  - School officials may require the information to perform their duties.
  - Faculty are considered advisors with legitimate educational need for their enrolled students, those seeking to enroll, or those they advise (IU Memo from Ken Gros Louis, May 1999).
- Parents of dependent students as claimed with the IRS (copy of tax form required)
- Lawfully issued subpoenas (University Counsel review and student notification required)
- Various authorized representatives of government entities (audits or evaluation of education programs, compliance with SEVIS, Solomon Amendment, etc.)
- Student signed consent to release

INDIANA UNIVERSITY
BLOOMINGTON

Third Party PIN Access

- Third-party access is a OneStart role that the student can assign to any person (such as a parent, guardian, or spouse)
- Student can allow third party access to the following information available in the Student Self-Service section: Holds on Record, Grades, Unofficial Transcript, Class Schedule, Final Exam Schedule, View and Download 1098-T, Financial Aid Award, Financial Aid Award Summary, Personal Info (Addresses, Phone Numbers, To do list)
- Remember, this access does not provide the right for discussion of the student restricted information with the third parties who have been provided this access
- Third Party Access Info http://kb.iu.edu/data/auoz.html#what

Release of Student Information Policy

Students have a right to know:

- What information from education records school officials within the institution can obtain *without obtaining prior written consent;*
- What the criteria are for determining who will be considered school officials;
- What kind of legitimate educational interest will entitle school officials to have access to education records;
- What information the institution has designated as public or directory information.
- Policy site:

http://policies.iu.edu/policies/categories/academic-faculty-students/university-student-services-systems/USSS-05-release-student-information.shtml

Restraint of Public Disclosure

- If a student does not want all or some of his/her directory information released to any person other than officials with legitimate need, he or she may complete and submit a restriction form to the Office of the Registrar.

- A complete restriction will block information from appearing in the online address book. Student names in ONCOURSE will be blocked from other students, unless the restricted student participates in chats/discussions.

- To remove the restriction, the student must complete a removal form and submit it to the Office of the Registrar.
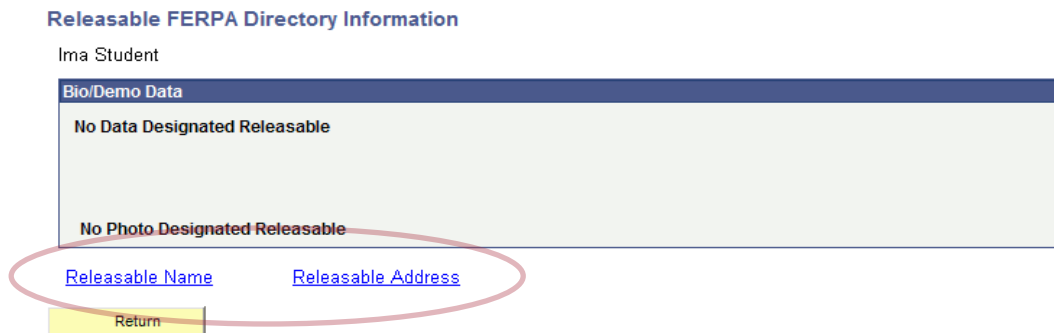
FERPA Restrictions in SIS

- If a student has filed a FERPA restriction, a window shade icon will appear in SIS:
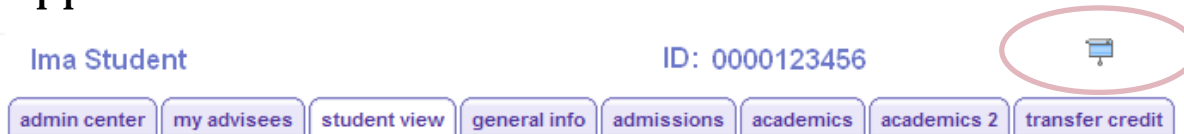
- When the icon is clicked, releasable information will appear in blue links under the BioDemo Data box:

2009 FERPA Regulation Highlights

- Biometric records have been added to the list of personal identifiers. Biometric records include records of biological or behavioral characteristics that can be used for automated recognition of an individual, including fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting.

- A directory exclusion does not give students the right to remain anonymous in class or to impede class communication.

- Institutions may release information when there are health and safety concerns. Exceptions for health concerns include serious communicable diseases, serious infectious diseases, and suicidal ideation. Information released should be documented.

- Under the Wetterling Act, FERPA allows an institution to disclose without consent information it has received from a State about a student who is required to register as a sex offender.

2009 FERPA Regulation Highlights, continued

- Institutions are now required to use "reasonable methods" to ensure that school officials obtain access **only** to those education records in which they have legitimate educational interests.

- Amended regulations require a school to use reasonable methods to **identify and authenticate** the identity of parents, students, school officials, and other parties before disclosing education records.

- FERPA prohibits the use of the Social Security number as an identification element when disclosing or confirming directory information.

- 2011 Rule – Allow states and agencies to share data more broadly for the purpose of tracking academic progress and evaluating educational programs.

2012 FERPA Regulation Highlights

- Expands definition of "authorized representative" to include entities conducting audits, evaluations, or compliance/enforcement activities.

- Clarifies that an education program means any program that is principally engaged in the provision of education, including but not limited to, early childhood education, elementary and secondary education, job training, career and technical education, and adult education, and any program that is administered by an educational agency or institution.

- Clarifies that displaying a student ID number on a student ID badge is acceptable, but only if the identified cannot be used to gain access to education records except when used in conjunction with one or more factor's that authenticate the user's identity.

- Clarifies that FERPA does not prevent a State or local educational authority or agency headed by an official listed in the Acts from entering into agreements with organizations conducting studies that would necessitate re-disclosing personally identifiable information from education records on behalf of educational agencies and institutions that disclosed the information to the State or local educational authority or agency .

2012 FERPA Regulation Highlights, continued

- Outlines that a State or local educational authority or agency headed by an official listed in the Acts is responsible for ensuring that its authorized representatives use personally identifiable information only to carry out audit or evaluation of education programs, to protect the information from further disclosure or other uses, and destroys the information when no longer needed for the purposes originally stated

- States that written agreements must be used to designate any authorized representative who is not an employee. The written agreement must specify:
    o The information to be disclosed;
    o The audit or evaluation purpose of the disclosure, and;
    o Require the destruction of the data when it has been used for the intended purpose

- Allows for an institution to specify that disclosure of directory information will be limited to specific parties, for specific purposes, or both. Any such limit on the use of directory information must be included in the institution's directory information notice to students.

Letters of Recommendation

- **Specific information** concerning academic performance (e.g., grades, ranking in class) requires release.

- If **personally identifiable information** is acquired from a student's education record, the writer is required to obtain signed release.

- Statements made from personal observation or knowledge do not require signed release. Mere observations about a student's behavior are not covered by FERPA because personal knowledge and observations are not derived from an "education record" subject to FERPA.

- As part of the education record, a student has the right to access letters of recommendation unless the student waives the right in writing.

FERPA & Reporting

Aggregate data reasonably reduces the risk of potentially identifying individuals.

- Sensitive data behind CAS authentication
- cell size <5 university standard (e.g., Grade Distribution Report)

Target Population

- Is there legitimate educational interest?
- Does the list only contain needed information (e.g., can UIDs be removed)?
- Are students with FERPA restrictions excluded from the population, especially if its end use is not academic business (e.g., mailing surveys to students)?
- Does the population of interest require use of sensitive data (e.g., country of citizenship)?

FERPA and Access

- Access based on the school official's "legitimate need to know"

- Technical measures must be used to restrict data based on legitimate need (FERPA 2009 Update)

- Here At IU...

    - Access Coordinators in each department validate employment and job requirements

        http://registrar.indiana.edu/reporting/data-access.shtml

    - Access Coordinators determine what access may be assigned in SIS, IUIE, and Workflow applications;

    - Data may be restricted to a department's majors and/or courses, depending on legitimate need.

Compliance and Training

- Acceptable Use Agreement https://protect.iu.edu/agreement

- FERPA Tutorial https://ferpa.iu.edu

- OTP Token

- Training Opportunities
  - Check out Registrar Website for Training information
    http://registrar.indiana.edu/reporting/training-resources.shtml
  - Check out SIS Training Website
    https://usss.iu.edu/sites/sistrainingsupport/default.aspx

Best Practices

- Never share your password

- Never login for anyone…even a student worker

- Lock system when stepping away from your desk

- Access only the information you need to do your job

- Use secure tools (Oncourse, SIS, etc..) provided by the university

- Don't store data on personal workstations, laptops, or mobile devices…*this includes USB drives*

- Know who has access to shared areas before sharing restricted data on network or SharePoint

- Box is not acceptable for any institutional data classified as "limited access/restricted" or "critical"

- Consider your wireless network

- Don't allow unauthorized individuals to view restricted data on your computer screen or mobile devices

- Don't talk with parents about their child's performance

Tips for Student Workers

- Keep OTP token locked in the office and give only when a task is required within SIS.

- Ensure compliance agreements are in place and the student understands privacy responsibilities.

- Remember to notify the Office of the Registrar when a student hourly is no longer employed, so access can be removed.

Tips for Faculty

- FERPA for Faculty web site: http://registrar.indiana.edu/policies/ferpa/student-privacy-faculty.shtml
- Use ONCOURSE to communicate about grades
- Previous academic performance of a student cannot be considered when assigning a grade.
- Consider your school's academic policy for grade changes, etc. when developing retention cycles for student records (e.g., roster, grades, papers) information that you maintain.
- Student education records are considered confidential and may not be released to third parties (including parents) without written consent from the student
- While grades can be submitted from a café in Paris, consider the security of your network.

Email Tips

Don't...

- o Send restricted information via e-mail
- o Send University ID in the subject line of an email
- o Send emails to the entire student population without getting prior approval [BFC Policy on Mass Email](#) [pdf]

Do...

- o Use ONCOURSE for posting or communicating grade information
- o Use Slashtmp (https://www.slashtmp.iu.edu) or Microsoft Lync when communicating with school officials about multiple students
- o Take appropriate action to secure sensitive data received through e-mail from parties not adhering to this practice

Your Role as Data Manager

If you handle student information, you have a data management role.

- Do you share student information with internal or external individuals on behalf of the university?
  - Is the recipient of that information aware of student privacy laws?
  - Is the recipient a school official and do they have a legitimate need to access the information?
  - Are safe data-handling practices in place when sharing the information?
- Do you manage a department system containing student information?
  - Are users aware of student privacy laws?
  - Have they taken the FERPA tutorial and signed the Acceptable Use Agreement?
  - Does their training include safe practices for handling data?

Tools and Resources

- Access Coordinators by department:

  http://registrar.indiana.edu/reporting/data-access.shtml

- Third Party PIN information:

  http://kb.iu.edu/data/auoz.html

- Training and resources for users with access to student records data:

  http://registrar.indiana.edu/reporting/training-resources.shtml

- Safe online practices and tools:

  http://protect.iu.edu

- Transferring files in a secure environment- use Slashtmp:

  https://www.slashtmp.iu.edu/

  Slashtmp documentation is available at http://kb.iu.edu/data/angt.html Podcast info at

  http://podcast.iu.edu/upload/UITS/bc7a4053-d601-4b76-8991-80ade8da609f/slashtmp.m4v

Tools and Resources, continued

- FERPA info online:

  http://registrar.indiana.edu/policies/student-privacy-ferpa.shtml

  - FERPA for Faculty, Staff, Parents, Students

  - FERPA tutorial

  - FERPA FAQ

  - IU Release of Student Information Policy

  - IUB Annual Notification of Student Rights

- Department of Education FERPA site:

  http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

- Indiana data protection laws FAQ

  http://protect.iu.edu/cybersecurity/data/laws

Err on the Side of Caution

If you are unsure…

… *Don't do it!!!*

Contact the Registrar first if you have any doubts.

We're happy to help!

Questions?