

FERPA Update: What You Need to Know...
FAEDS 2009 Annual Conference
Orlando, Florida
September 28-30, 2009

Bill Mullooney
Vice President for Policy and General Counsel
Valencia Community College

*- 15 YRS
24 YRS ED LAW*

Federal Law: FERPA Background and Basics

The Family Educational Rights and Privacy Act of 1974 ("FERPA"), § 513 of P.L. 93-380 (The Education Amendments of 1974), was signed into law by President Ford on August 21, 1974, with an effective date of November 19, 1974, 90 days after enactment. FERPA was enacted as a new § 438 of the General Education Provisions Act (GEPA) called "Protection of the Rights and Privacy of Parents and Students," and codified at 20 U.S.C. § 1232g. It was also commonly referred to as the "Buckley Amendment" after its principal sponsor, Senator James Buckley of New York. This is the keystone privacy and access law for educational institutions. This law (and similar Florida laws, s. 1002.22, 1006.52, 1002.221, 1002.225 F.S.), provides a cluster of rights to students, including the right of access, the right of waiver of access to confidential letters or statements, the right to challenge and hearing, and the right of privacy. Applies with equal force to electronic records as it does to paper records. These rights continue to exist after the student's graduation and expire only upon the student's death.

- A. Information related to a student that is maintained within a college computer system, which does not fall within any of the listed exceptions, meets the definition of "education records" under FERPA. The determination of what is or is not an "education record" for purposes of FERPA hinges solely on the statutory definition, which, under long-standing FPCO interpretation, is quite broad: a "record" (a term that is itself defined quite broadly) is an "education record" if it is "1) directly related [that is, "personally identifiable"] to a student; 2) maintained by an educational agency or institution, or a party acting for the agency or institution; and 3) not excluded from the definition [under one of several specific and limited exceptions]".
- B. If there is a complaint that someone accessed education records inappropriately using a computerized student information system, and the school does not have a system that allows the school to know who accesses records, then the school has a policy or practice of permitting access to education records without knowing whether the school official has a legitimate educational interest in those records (violation of FERPA). The system has got to be one that permits the institution to know who is accessing records.
- C. **Definitions:**
 - a. **"Educational institution":** "any public or private . . . institution" that receives funds "under any program administered by the Secretary [of Education]".
34 C.F.R. §§ 99.1 and 99.3.

*APPLIES TO
REG RECEIVING
FEDERAL FUNDS.*

- b. **“Record”**: “any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche”. 34 C.F.R. § 99.3. In 1996, the term “record” was amended to add “computer media” to the definition of record. Email messages may fall within the definition of “education records” provided the message is “maintained” by the institution. Issues: Number of electronic records is huge – retention a problem. Note: FERPA applies only to records and information taken from records; it does not apply to unrecorded information. “Nothing in FERPA prohibits a school official from disclosing . . . information that is based on that official’s personal knowledge or observation and not from an education record”.\
- c. **“Student”**: “any individual who is or has been in attendance at an educational . . . institution”. 34 C.F.R. § 99.3. The term does not include applicants, who thus are not protected by FERPA unless and until they are admitted and “attend”, thereby becoming “students”. If they do, however, FERPA “reaches back” and brings their application records within its scope.
- d. **“Attendance”**: “includes, but is not limited to . . . attendance in person or by correspondence”. 34 C.F.R. § 99.3.
- e. **“Directly related”**: The term is not defined in either the statute or the regulations, but, under long-standing interpretation of the Family Policy Compliance Office, the office within the Department of Education charged with overseeing FERPA, a record is considered to be “directly related” to a student if it contains “personally identifiable information” about that student.
- f. **“Personally identifiable information”**: “includes, but is not limited to:
 - (i) The student’s name;
 - (ii) The name of the student’s parent or other family member;
 - (iii) The address of the student or student’s family;
 - (iv) A personal identifier, such as the student’s social security number or student number;
 - (v) A list of personal characteristics that would make the student’s identity easily traceable; or
 - (vi) Other information that would make the student’s identity easily traceable.”
- g. **“Maintained”**: A record is “maintained” by an educational institution whenever it is in the possession, custody, or control of any employee or agent of the institution.

D. The only such records that are specifically excluded from the scope of the term, and that therefore are not subject to the restrictions of FERPA, are the following:

- a. **“Sole possession” records**: “Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record.” 34 C.F.R. § 99.3.
- b. **“Law enforcement” records**: those records that are “(i) created by [the institution’s] law enforcement unit [including non-commissioned public safety or security offices]; (ii) created for a law enforcement purpose; and (iii) maintained by the law enforcement unit.” 34 C.F.R. §§ 99.3 and 99.8

- c. **“Employment” records:** records related solely to the employment of a “student” by the institution, provided that the student is not “employed as a result of his or her status as a student”. 34 C.F.R. § 99.3.
- d. **“Treatment” records:** records that are “(i) made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity; (ii) made, maintained, or used only in connection with treatment of the student; and (iii) disclosed only to individuals providing the treatment.” 34 C.F.R. § 99.3.
- e. **“Alumni” records:** “Records that only contain information [obtained] about an individual after he or she is no longer a student at that agency or institution”. 34 C.F.R. § 99.3. If the information recorded “relates back” to the student’s time at the institution, it is still an “education record” even though it was generated after its subject was no longer a “student”.

E. Disclosure

- a. **With Consent:** In general, an institution cannot disclose “education records” – or information from “education records” – to anyone other than the relevant student unless it first has obtained a signed and dated written consent from the relevant student (or *all* relevant students, if the records are “directly related” to more than one), specifying the records that may be disclosed, the purpose for which they may be disclosed, and the persons or classes of persons to whom they may be disclosed. 34 C.F.R. § 99.30(a) and (b).

Without Consent (*Each of these exceptions is independent of the others. As far as FERPA itself is concerned, it is entirely within the institution’s discretion whether to make a disclosure under any of these exceptions - except in the K-12 institutions, where parents are granted rights. Thus, for example, a parent never has a right, under FERPA, to see his or her college student’s education records, even if the student is the parent’s dependent for tax purposes, is involved in a health or safety emergency, and has violated the institution’s alcohol policies – and even if the student is not yet 18 years old. A subpoena, a court order, or another law such as the Campus Sexual Assault Victims’ Bill of Rights Act may require disclosure in certain circumstances, but FERPA does not.*)

- i. Directory information (*DETERMINED BY INST.*)
- ii. School officials with legitimate educational interests *- LISTED IN ANNUAL NOTIFICATIONS*
- iii. The disclosure is to another educational institution where the student seeks or intends to enroll.
- iv. The disclosure is to the student him- or herself. (*OR PARENT ≤ 18 yrs old*)
- v. The disclosure is to parents of a student who is considered their “dependent” for federal tax purposes. (*STUDENT*)
- vi. The disclosure is made “in connection with a health or safety emergency”, is made only to “appropriate parties”, and is limited to information that “is necessary to protect the health or safety of the student or other individuals”.

- vii. The disclosure is made to “comply with a judicial order or lawfully issued subpoena”.
- viii. The disclosure is to a court in the context of a lawsuit that the student brought against the institution or that the institution brought against the student.
- ix. The disclosure is to parents of a student who is under the age of 21 at the time of the disclosure and relates to a determination by the institution that the student has violated its drug or alcohol rules.
- x. The disclosure is of the “final results” of a disciplinary proceeding against a student whom the institution has determined violated an institutional rule or policy in connection with alleged acts that would, if proven, also constitute a “crime of violence or non-forcible sex offense”.
- xi. The disclosure is to “a victim of an alleged perpetrator of a crime of violence or non-forcible sex offense” and consists only of the “final results” (as defined above) of an institutional disciplinary proceeding in connection with that alleged crime or offense. The institution may (and, under the Campus Sexual Assault Victims’ Bill of Rights Act, must) make such a disclosure regardless of the outcome of the proceeding.
- xii. The disclosure is in connection with financial aid that the student has applied for or received and is for the purpose of determining the student’s eligibility for, the amount of, or the conditions for the aid, or to enforce the terms and conditions of the aid.
- xiii. The disclosure is to authorized representatives of the Comptroller General, Attorney General, Secretary of Education, or state or local educational authorities in connection with an audit of federal- or state-supported education programs or with the enforcement of or compliance with federal legal requirements relating to those programs. In the absence of consent or a specific federal law to the contrary, information collected under this exception must be protected so that individuals are not personally identifiable other than to the “authorized representatives”, and the information must be destroyed when no longer needed.
- xiv. The disclosure is to accrediting organizations to carry out their accrediting functions.
- xv. The disclosure is to organizations conducting studies for educational institutions to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction, provided that the studies are conducted in a manner that prevents personal identification of parents and students by anyone other than representatives of the organizations and the information is destroyed when no longer needed for purposes of the studies.

F. Redisclosure

- a. FERPA imposes similar limitations on redisclosure. In general, an institution disclosing personally identifiable information from an education record must inform the recipient that it cannot redisclose that information without the consent

of the student and that it may use the information only for the purpose for which the disclosure was made. 34 C.F.R. § 99.33(a). Exceptions to this requirement include disclosures of directory information; disclosures to the relevant student, to the parents of a dependent student, or to parents in connection with a drug or alcohol violation; and disclosures made in connection with a court order, lawfully issued subpoena, lawsuit in which the student and the institution are adversaries, or disciplinary proceeding involving an alleged crime of violence or non-forcible sex offense.

G. Recordkeeping

- a. The institution generally must maintain a record of each request for access to and each release of personally identifiable information from a student's education records. This separate record must include, at a minimum, the identities of the requesters and recipients and the "legitimate interests" they had in the information. It also must be maintained with the student's education records for as long as those records are themselves maintained. Exceptions to this requirement include disclosures to a school official, a parent or student, a person with written consent, or a person requesting directory information, and disclosures in connection with a grand jury or other law enforcement subpoena prohibiting disclosure of its existence or contents.

H. Inspection and Review

- a. The institution must provide access to the records within 45 days of a request and must respond to reasonable requests for explanations and interpretations of the records. FERPA does *not* require the institution to provide copies of records to the student, unless "circumstances effectively prevent" the student from exercising the right to inspect and it is not possible to "make other arrangements" for inspection.

I. Amendment

- a. If a student believes that his or her education records contain inaccurate or misleading information or information that violates the student's right to privacy, the student may request that the institution amend the records. The institution must make a decision on the request within a "reasonable time" after receipt. If the institution decides not to make the requested amendment, it must so inform the student and advise the student of the right to a hearing. The courts have ruled that this portion of FERPA is intended to deal with "scrivener's errors", not to provide a means by which a student may challenge substantive decisions, such as grades, or obtain information on how a particular grade was assigned.

J. Annual Notification of Rights

- a. FERPA requires each institution to notify its students annually of their rights under the act.

K. Enforcement

- a. The responsibility for enforcing FERPA rests with the Family Policy Compliance

Office of the Department of Education, which is authorized to investigate and review potential violations and to provide technical assistance regarding compliance issues. State law provides for a private right of action (no private right of action under federal law), affirmative disclosures of educational records are traditional complaint – possible to read FERPA to impose liability if institution fails to protect information and it is released (negligence). The prohibition against “disclosures” extends not only to intentional, affirmative acts of disclosure, but also to inadvertent disclosures, and even to an unclear degree to unintentional “failures” to take “reasonable” and “appropriate” measures to protect “education records” from unauthorized access. “It should be noted that ‘disclosure’ not only means the transmitting or releasing of information to a third party but encompasses *permitting* a third party to have access to the information in *any* manner, including oral, written, or electronic means.”

Recent Changes in Florida Law

- A. Students’ right to access and right to privacy with regard to education records is a critical issue for higher education institutions in terms of institutional operations, not to mention campus safety and security. Due to years of inattention, Florida’s analogy to FERPA, formerly codified in Florida Statutes as s. 1002.22, stagnated as the federal law evolved and responded to emerging needs. This resulted in numerous inconsistencies between Florida and federal law that often placed educational institutions in the untenable position of making decisions about the disclosure of student education records that may have comported with federal FERPA, but not with the Florida statute.
- B. The most critical inconsistencies, now eliminated, between Florida law and federal law were:

Applicant Records. Both Florida and Federal law excluded applicants who do not enroll from their respective definitions of “student” for purposes of the provision of access and other rights. Therefore, under FERPA, no person, including applicants, has the right to access applicant records. However, under Florida law, applicant records arguably could have been accessed by any person via a public records request, as applicant records were not made confidential and exempt from sec. 119.07(1). This was a glitch that could have been read to place academic transcripts, disability records, and other confidential information in the public domain.

Directory Information. In specifically excluding “directory information” from the definition of “record,” State law blatantly conflicted with federal law, which considers directory information to be education record, albeit of a non-invasive nature. Directory information was arguably public record information pursuant to Florida law. Schools were forced to violate FERPA opt out requirements to comply with state public records law.

Litigation. In the absence of specific FERPA tracking language in the prior state law, the release of records without written consent in the event an educational

agency or institution initiated legal action against a parent or student, or when a parent or eligible student initiated legal action against an educational agency or institution, would have been prohibited under state law – a nonsensical outcome.

Federal Grand Jury and Law Enforcement Subpoenas. Not allowed under prior state law, while authorized under FERPA and required by other law or regulation.

Disclosure to Victim of Crime of Violence. Not allowed under prior state law, while authorized under FERPA and required by other law or regulation.

Disclosure of Records concerning Registered Sex Offenders. Not allowed under prior state law, while authorized under FERPA and required by other law or regulation.

Disclosure for Order in Case of Terrorism. Not allowed under prior state law, while authorized under FERPA and required by other law or regulation.

Statute of Limitations. No stated time limit for bringing an action under prior state law, while FERPA provides, “[a] timely complaint is defined as an allegation of a violation of the Act that is submitted to the Office within 180 days of the date of the alleged violation or of the date that the complainant knew or reasonably should have known of the alleged violation.”

- C. During the 2009 Legislative session, the Board of Governors, the State University System, the Florida College System, and the Florida Department of Education supported amendments to Florida’s student education records laws to eliminate the foregoing and other inconsistencies with FERPA and provide clarity to Florida’s public postsecondary institutions and their students. House bills 7117 and 7119 incorporated these amendments and became law on July 1, 2009.
- D. Florida’s new education records laws specify that the rights of students and parents with regard to education records are protected in accordance with FERPA, thus ensuring that state law is always consistent with FERPA. Also, education records, as defined by FERPA and not state law, are confidential and exempt from the Florida’s public records laws. Finally, for public postsecondary institutions, applicant records are confidential and exempt from the Florida’s public records laws.



The Final Federal Regulations: Changes in Institutional Practice/Policy

- Update your annual FERPA notice or FERPA policy to ensure that your definition of “school official” is broad enough to include contractors, consultants, volunteers and other outside parties providing services and functions or otherwise acting for an agency or institution.

▶ Also add text to clarify that the school forwards education records to schools in which the student seeks to enroll (or is enrolled) so long as the disclosure is for purposes related to enrollment or transfer. Clarify that sending information to a school where student seeks to enroll may include updated or corrected information. This includes disciplinary and health records, with the caveat that it must be related to the student's enrollment or transfer.

▶ Include information security language in all contracts with outside contractors to ensure safeguarding of education records that are under their care, in an attempt to meet the direct control standard in the new regulations. See sample data security language section.

*SEE SAMPLE
ON LAST PG.*

▶ On direct control, consider other ways to verify data security practices of outside contractors. For example, if education records will be sent to an outside contractor, consider a physical review of contractor's site and data security (including any subcontractors).

▶ Note that institutions can rely upon a student's assertion that he/she is a dependent for tax purposes. Initiate a process on campus for capturing this information. See model forms at <http://www.ed.gov/policy/gen/guid/fpco/ferpa/safeschools/modelform.html> and <http://www.ed.gov/policy/gen/guid/fpco/ferpa/safeschools/modelform2.html>

▶ Review institutional practices and software available for controlling access to education records by school officials. Consider physical or technological controls where possible, and administrative controls where physical/technological controls are not possible. For example, does the software the school uses contain role based security features that allow professors to only view information about students in their class? If not, discuss what steps might be taken to move toward this type of control. Review grant of access by role, not only by page view but by queries submitted to the system.

▶ Review situations where email containing sensitive data (e.g. you are in danger of receiving a failing grade) is sent to multiple students. Train administrators on how to set up a listserv protecting the identity of recipients or properly use the blind cc field so that inadvertent data releases do not occur. Consider role based limitations on who may send emails with sensitive data.

▶ In terms of de-identified data that is released, review the strategy for ensuring data releases of de-identified data do not inadvertently contain data that can be aggregated in such a manner as to reveal identities. This applies to sequential disclosures. Add a sentence to school's student record policy as needed to clarify that schools (and their vendors) may not use an SSN or other non-directory information, either alone in or combination with other data elements, to identify student records when disclosing or confirming directory information w/o written consent from the student.

▶ Clarify (if the school wishes to) that parents of a student are appropriate parties to whom schools may disclose information without consent in a health or safety emergency, even if students are not dependents for tax purposes.

- ▶ Review methods for authenticating the identity of those requesting release of information. Clarify that schools may not require the accuser to execute a non-disclosure agreement or otherwise interfere with re-disclosure of information about alleged sex offenses released under the Clery Act.
- ▶ Amend definition of directory information on student ID number. A “Student ID Number” is a student ID number, user ID, or other unique personal identifier used by the student for purposes of accessing or communicating in electronic systems, but may be included in your definition of directory information only if the identifier cannot be used to gain access to education records except when used in conjunction with one or more factors that authenticate the user’s identity.
- ▶ Add sentence to policy clarifying that disclosure w/o consent is allowed when the school is returning records to the apparent creator (e.g. of a transcript) to verify authenticity.
- ▶ Update definition of education records to clarify when peer-graded papers become an education record (before they are “maintained” by the institution).
- ▶ Clarify (if necessary) that, with respect to former students, the term “education records” excludes records that are created or received by the organization after an individual is no longer a student in attendance and are not directly related to the individual’s attendance. Update definition of personally identifiable information if your policy includes that terminology.
- ▶ Draft a model written agreement to be used with organizations conducting studies for or on behalf of the institution for purposes of testing, student aid and improvement of instruction. The agreement must specify the purposes of the study, and that education records may only be used for the stated purpose(s). Agreement must contain restrictions on re-disclosure and destruction of information once study is complete.
- ▶ If your policy states that disclosure in a health or safety emergency is to be strictly construed, amend it to include new text in final rule, which is as follows: The school may disclose education records if it determines that there is a articulable and significant threat to the health or safety of a student or other individuals, but only to those persons whose knowledge of the information is necessary to protect the health or safety of the student or other individuals. Add note that a record must be kept of the threat and the parties to whom the information was disclosed.
- ▶ Clarify that the school may disclose information received under a community notification program about a student who is required to register as a sex offender.
- ▶ Put a procedure in place for recording names of State and local educational authorities and federal officials and agencies under 99.31(a)(3) that may make further disclosures without consent, and obtaining a copy of the record of further disclosures.

Model Notification of Rights under FERPA for Postsecondary Institutions

The Family Educational Rights and Privacy Act (FERPA) affords students certain rights with respect to their education records. These rights include:

(1) The right to inspect and review the student's education records within 45 days of the day the College receives a request for access.

A student should submit to the registrar, dean, head of the academic department, or other appropriate official, a written request that identifies the record(s) the student wishes to inspect. The College official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the College official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.

(2) The right to request the amendment of the student's education records that the student believes are inaccurate, misleading, or otherwise in violation of the student's privacy rights under FERPA.

A student who wishes to ask the College to amend a record should write the College official responsible for the record, clearly identify the part of the record the student wants changed, and specify why it should be changed.

If the College decides not to amend the record as requested, the College will notify the student in writing of the decision and the student's right to a hearing regarding the request for amendment.

Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.

(3) The right to provide written consent before the College discloses personally identifiable information from the student's education records, except to the extent that FERPA authorizes disclosure without consent.

The College discloses education records without a student's prior written consent under the FERPA exception for disclosure to school officials with legitimate educational interests. A school official is a person employed by the College in an administrative, supervisory, academic or research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the College has contracted as its agent to provide a service instead of using College employees or officials (such as an attorney, auditor, or collection agent); a person serving on the Board of Trustees; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks. A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibilities for the College.

[Optional] Upon request, the College also discloses education records without consent to officials of another school in which a student seeks or intends to enroll. [NOTE: FERPA requires an institution to make a reasonable attempt to notify each student of these disclosures unless the institution states in its annual notification that it intends to forward records on request.]

(4) The right to file a complaint with the U.S. Department of Education concerning alleged failures by the College to comply with the requirements of FERPA. The name and address of the Office that administers FERPA is:

Family Policy Compliance Office
U.S. Department of Education
400 Maryland Avenue, SW
Washington, DC 20202-5901

[NOTE: In addition, an institution may want to include its directory information public notice, as required by § 99.37 of the regulations, with its annual notification of rights under FERPA.]

Data Security Terms for inclusion in Contracts with Service Providers
Protection of Confidential Data

Service Provider agrees to abide by the limitations on re-disclosure of personally identifiable information from education records set forth in The Family Educational Rights and Privacy Act (34 CFR § 99.33 (a)(2)) and with the terms set forth below. 34 CFR 99.33 (a)(2) states that the officers, employees and agents of a party that receives education record information from the Institution may use the information, but only for the purposes for which the disclosure was made.

Definition: Covered data and information (CDI) includes paper and electronic student education record information supplied by Institution, as well as any data provided by Institution's students to the Service Provider.

Acknowledgment of Access to CDI: Service Provider acknowledges that the Agreement allows the Service Provider access to CDI.

Prohibition on Unauthorized Use or Disclosure of CDI: Service Provider agrees to hold CDI in strict confidence. Service Provider shall not use or disclose CDI received from or on behalf of Institution (or its students) except as permitted or required by the Agreement, as required by law, or as otherwise authorized in writing by Institution. Service Provider agrees not to use CDI for any purpose other than the purpose for which the disclosure was made.

Return or Destruction of CDI: Upon termination, cancellation, expiration or other conclusion of the Agreement, Service Provider shall return all CDI to Institution or, if return is not feasible, destroy any and all CDI. If the Service Provider destroys the information, the Service Provider shall provide Institution with a certificate confirming the date of destruction of the data.

Remedies: If Institution reasonably determines in good faith that Service Provider has materially breached any of its obligations under this contract, Institution, in its sole discretion, shall have the right to require Service Provider to submit to a plan of monitoring and reporting; provide Service Provider with a fifteen (15) day period to cure the breach; or terminate the Agreement immediately if cure is not possible. Before exercising any of these options, Institution shall provide written notice to Service Provider describing the violation and the action it intends to take. If the Family Policy Compliance Office of the U.S. Department of Education determines that the Service Provider improperly disclosed personally identifiable information obtained from Institution's education records, Institution may not allow the Service Provider access to education records for at least five years.

Maintenance of the Security of Electronic Information: Service Provider shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted CDI received from, or on behalf of Institution or its students. These measures will be extended by contract to all subcontractors used by Service Provider.

Reporting of Unauthorized Disclosures or Misuse of Covered Data and Information: Service Provider shall, within one day of discovery, report to Institution any use or disclosure of CDI not authorized by this agreement or in writing by Institution. Service Provider's report shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the CDI used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure, (iv) what Service Provider has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Service Provider has taken or shall take to prevent future similar unauthorized use or disclosure. Service Provider shall provide such other information, including a written report, as reasonably requested by Institution.