2009 FERPA Amendments

A Compliance Guide for Minnesota State Colleges and Universities

Chief Academic and Student Affairs Officers and Deans Conference

May 28, 2009

Office of General Counsel

On December 9, 2008, the Department of Education ("Department") published its final changes to the Family Educational Rights and Privacy Act (FERPA) regulations, 34 CFR Part 99. The following link will take you to the Family Policy Compliance Office's (FPCO) *Dear Colleague Letter* that provides a summary of the amendments and links to additional detailed resources: a pdf copy of the final regulations; and a section-by-section analysis. http://www.ed.gov/print/policy/gen/guid/fpco/hottopics/ht12-17-08.html . Some of the amendments represent change in interpretation, some are clarifications of best practices, and some codify interpretations already taken by the Family Policy Compliance Office in advisory letters.

To assist system colleges and universities in implementing the new regulations, the Minnesota State Colleges and Universities Office of General Counsel offers the following compliance guide for issues related to student affairs. Note this does not cover all aspects of the amendments, particularly as related to disclosures to other government entities and research organizations.

Please contact the Office of General Counsel, Kris Kaplan, Kristine.kaplan@so.mnscu.edu, 651 296-3905, or a member of the Education Division of the Attorney General's Office for additional information or assistance.

I. Review Campus FERPA Policies and Procedures

Each college and university must have a published campus FERPA Policy that, at a minimum, include the basic notice requirements of federal law; *see* FPCO model notice: http://www.ed.gov/policy/gen/guid/fpco/ferpa/ps-officials.html Additionally, system colleges and universities are strongly urged to have written policies and procedures to address various discretionary matters on handling its educational records. Several of the 2009 FERPA amendments pertain to these discretionary practices and should be reviewed as the FPCO has reinforced the importance of notifying students of the college or university's practices and documenting the basis for disclosures.

A. Health and Safety Emergency Disclosures

1. **The Amendments:** The "strict construction" language is removed and new wording clarifies that disclosure is permitted if there is an "articulable and significant" threat to the health or safety of a student or other individual. If so, information from *any* education record necessary under the circumstances may be disclosed to appropriate parties (including but not limited to parents, potential victims or any person whose knowledge of the information is needed) to protect the health or safety of the student

or others. *New:* colleges and universities must record and retain certain information concerning the circumstances of the emergency.

2. **Steps to Take:** Establish or revise campus procedures for handling health or safety emergencies to include decision making on release of education records. The procedure should reference the "articulable and significant" threat standard and factors for identifying an "appropriate party" to whom disclosure may be made (including parents, law enforcement and others). Provide training to frontline administrators who are most likely to have to exercise appropriate judgment on determining whether a health or safety emergency exists. The procedure must also include the creation and maintenance of a record that includes: the threat, a description of the records that were disclosed and to whom the disclosure was made. Records should be created as soon as practicable under the circumstances.

B. **Directory Information**

1. **The Amendments.**
   a. The Department codified previous advice that **electronic personal identifiers** may be classified as (public) directory information so long as such an identifier cannot be used by itself to access private data (and is not a SSN in whole or in part).
   b. **Opt-Out Procedures:** Regulations clarified to provide that an enrolled student's decision to "opt-out" of making his/her directory information public must be honored after the student leaves unless the student rescinds the decision; clarified to state that the right to "opt-out" of public directory information does not guarantee the student's anonymity in class – whether conducted in person or online.
2. **Steps to Take.**
   a. Review campus definition of directory information and determine whether to include electronic personal identifiers such as e-mail addresses or tech ID numbers – permissible so long as PIN or private access code is required to access other private data.
   b. Include information on procedures for suppressing or opting-out of public directory information in published FERPA Policy and advise students of process (and potential consequences) as part of orientation; advise students intending to enroll in online courses that their e-mail addresses will be available to other students and to find an alternative course or section if that is a concern.

C. **Post-Enrollment (Alumni) Records**

1. **The Amendments**. Clarified that only records about a former student that are unrelated to his/her activities as an enrolled student may be classified as "alumni records" (and therefore not subject to FERPA). Note that colleges and universities are not required to permit former students to suppress their directory information after they are no longer enrolled.
2. **Steps to Take.** Review campus procedures related to handling data about former students to accurately determine whether it is an educational or alumni record and appropriately consider a request to suppress directory information.

D. **Disclosing Education Records to Other Schools**

1. **The Amendments.**
    a. **May Disclose at Any Time to Other Colleges and Universities.** Changed previous limitation on disclosing education records without the student's consent only at the time the student signifies his/her intent to enroll or transfer to permit disclosure at any time so long as for purposes related to the student's enrollment or transfer. Comments clarify that any education records may be disclosed to the new school, including records of discipline, but caution that health-related education records should be sent separately to ensure compliance with any other applicable laws and after admission in order to ensure that decisions are not based on improper factors.
    b. **May Return Records to Original Provider or Creator.** Amended the definition of "disclosure" to exclude returning an education record or information from an education records to the party identified as the provider or creator of the record. (Generally the originator will be another school, but could be any third party provider.)
2. **Steps to Take.**
    a. Amend campus FERPA policy to state practice of disclosing education records, as appropriate, to other colleges or universities where the student intends to or has enrolled (at any time), and revise implementing procedures as necessary, including supplements, updates or corrections to any records previously sent. If policy does not mention these disclosures, then school must make reasonable efforts to notify student unless disclosure was initiated by the student.
    b. Amend campus procedures to permit returning education records to the original source of the record for appropriate purposes, such as verification of authenticity.

E. **Outside Service Providers as "School Officials" ("Out-Sourcing")**

1. **The Amendments.** Clarified that "school officials" (who may have access to private education records without the student's consent for "legitimate educational interests") may include contractors, consultants, volunteers, and other outside service providers used by the college or university to perform institutional services and functions. The college or university remains responsible for the privacy and security of the records in the third party's hands. The third party must be under the "direct control" of the college or university re: maintenance and use of data, including re-disclosure regulations.
2. **Steps to Take.** Review FERPA policy to ensure that contractors, consultants, volunteers and other service providers are included in definition of "school officials;" review procedures to ensure that outsourced services are limited to those that would otherwise be performed by employees; perform appropriate "due-diligence" to review security and privacy practices of outside service providers; use OGC/AGO-approved contract provisions to ensure that the college or university retains *direct control* over the contractor's maintenance, use and disclosure of education records provided to outside service providers: require agreement that the information may be used only for the purposes for which the records were disclosed, access is permitted only by individuals with legitimate educational interests (as determined by the college or university), and no re-disclosure of personally identifiable information is permitted from the education

records except as authorized by the student or college or university, consistent with FERPA. *See* Sample Agreement Terms.

F. **Reasonable Methods to Control Access to Records.**

1. **The Amendments.** Added specific requirement that colleges and universities use "reasonable methods" to ensure that school officials (including outside service providers) obtain access to only those education records – paper or electronic – in which they have legitimate educational interests. In a related amendment, the regulations now require colleges and universities to use reasonable methods to *identify and authenticate* the identity of parties to whom education records are disclosed.
2. **Steps to Take.** Reassess administrative, technological and physical measures employed on campus to appropriately restrict access and determine whether additional controls or training is needed; perform appropriate "due-diligence" to review security and privacy practices of outside service providers. The appropriate measures of control will depend on the risk of unauthorized access, i.e., the likelihood the records will be targeted for compromise and the potential harm. Institute training, as appropriate, to ensure notice and understanding of record handling responsibilities. Implement reasonable methods of identification and authentication that do not employ widely available information such as name, DOB, student ID number, etc. and NEVER Social Security Number (unless the student has specifically consented in writing).

G. **De-identified Records.**

1. **The Amendment.** Education records may be released without consent if all personally identifiable information has been removed. The regulations were amended to clarify that personally identifiable information includes "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."
2. **Steps to Take.** Colleges and universities should institute practices to ensure that individuals releasing redacted or aggregate information from education records consider the possibility of "implicit" data releases through such means as: use of other information that is widely available in the school community that could be linked to identify the student; a request that is targeted to an individual; or reporting on such a small cell of individuals that a student could be identified.

H. **Other Authorized Disclosures.**

1. **The Amendments.** The regulations now recognize the effect of other federal laws that permit the disclosure of information from education records under certain circumstances. First, without consent or notice to a student, colleges and universities are now explicitly permitted to disclose education records in response to an *ex parte* court order from the U.S. Attorney under the USA Patriot Act. Second, the regulations now permit a college or university to disclose any information that it has received from a state law enforcement agency about a student who is required to register as a sex offender. Third, the regulations now codify FPCO guidance that colleges and universities may not prohibit victims of "crimes of violence or non-forcible sex offenses" from re-disclosing disciplinary information they receive under the Clery Act.

2. **Steps to Take.** Consistent with general practices, a system college or university that receives a subpoena or court order purported to be issued under the USA Patriot Act should immediately contact an attorney in the Office of General Counsel or the Attorney General's Office for assistance. Consultation with the OGC or AGO is highly recommended before notifying the campus community of a student who is a sex offender. Determining the extent and content of each notice requires a careful balance of privacy and safety concerns as well as compliance with state law and the notice guidelines issued by the U.S. Attorney, which were published in the *Federal Register* on Jan. 5, 1999 (64 FR 572) and Oct. 25, 2002 (67 FR 65598). Before disclosing student disciplinary information to the victim of a "crime of violence or non-forcible sex offense" (*see* System Procedure 1B.3.1.) consult with the OGC or AGO to ensure that only appropriate information is provided.

II. CLASSROOM ISSUES

A. "Students" Defined. Colleges and universities may wish to amend their policies and/or remind faculty and staff that all individuals receiving educational services, by any method including online, are "students" whose records are subject to FERPA and state privacy laws. Provide training or tips on avoiding inadvertent data releases and protecting the identity of e-mail recipients by the use of listservs or the blind copy feature.

B. Peer-graded Papers. Colleges and universities may wish to amend their definition of education records to clarify that student-produced documents, including peer-graded papers or group projects, do not become "education records" until they are "maintained" by the college or university; generally, this would occur at the time the paper or project is collected by the instructor.

C. Posting Grades. While not recommended, faculty could publicly post course grades using randomly generated numbers that are used only for the course and the "key" is available only to the course instructor. Posting grades by a student ID number that is widely available or a partial SSN is NOT permitted.

D. ID in Class. Students do not have the "right" to remain anonymous in class – whether the course is conducted in person or online – even if the student has requested suppression of his/her directory data. Students who do not wish to reveal their e-mail address or other electronic identifier that must be used to participate in an online course should be advised to find a different section of the course.