INTRODUCTION:

A little over one year ago, the U.S. Department of Education ("Department") published final new regulations [1] under the Family Educational Rights and Privacy Act ("FERPA" or "Act"). The new rules were developed in large part to respond to the growing use of statewide longitudinal data systems ("SLDS") and other data sharing programs that track student and educational program outcomes and success. Specifically, the Department stated that the amendments were needed to ensure that the Department continues to protect the privacy of education records while allowing for the effective use of data. [2] Improved access to data in SLDS, the Department noted, will facilitate a state’s ability to evaluate education programs, ensure limited resources are invested effectively, build upon what works, increase accountability and transparency, and contribute to a culture of innovation and continuous improvement. [3]

While these purposes are laudable when viewed in isolation, not everyone agrees that the amendments to the regulations are appropriate or consistent with FERPA. Those skeptical of the regulations warn that they effectively reduce the privacy of student education records and allow state and local educational authorities, as well as authorized representatives of the Comptroller General, Secretary, and Attorney General, [4] substantially greater access to personally identifiable information in education records (without the consent of the student) [5] than under prior rules [6] and interpretations. Within two months of the effective date of the regulations, the Electronic Privacy Information Center ("EPIC") and others challenged the regulations in federal court in the District of Columbia under the Administrative Procedure Act, asserting the regulations are not in accord with law and in excess of statutory authority. [7] While questions exist regarding the validity of these regulations, they nevertheless remain in effect and institutions can rely on them until a court rules otherwise.

Part I of this Note summarizes the major changes included in the amended regulations. These include new definitions and revised interpretations, a relaxed view of the legal authority required to gain access to student education records, the expansion of the audit and evaluation and studies exceptions, [8] the broadening of authority to re-disclose information, and the expansion of enforcement authority. Part II discusses State Longitudinal Data Systems ("SLDS") [9] in the context of higher education, and Part III provides a checklist of terms to include in SLDS data-sharing agreements, as well as terms for agreements involving the studies exception, and the audit and
DISCUSSION:

I. Summary of Major Changes in the December 2, 2011 Regulations

A. In General

As a preliminary matter, FERPA does not grant authority to the federal government or others to collect data. Nor does it require an institution of higher education to disclose personally identifiable information. Rather, FERPA is a conditional funding law that prohibits federal education funding to educational agencies or institutions unless certain policies involving inspection, review, access, and protection of student education records are in place. The Act addresses two key issues: (1) the right of a student to review and seek correction of his education records; and (2) the disclosure of personally identifiable information from such records.

The new regulations allow authorities to more easily share and re-disclose data from student education records for purposes of audits, evaluations, and studies. In so doing, the amended rules also reduce certain privacy protections in the name of effective use of data and increased accountability and transparency. In that vein, a private postsecondary institution may disclose personally identifiable information from education records, without consent, to a school district about the district’s former students who are now in attendance at the private university, for the purpose of the district evaluating the federal or state-supported education programs the district administers. In a similar manner, a state postsecondary data system may re-disclose personally identifiable information from the system, without consent, to a state department of education in connection with an evaluation of whether the school districts in the state effectively prepared their graduates to enroll and succeed in postsecondary education.

B. Definitions

The amended regulations define, redefine, or provide new interpretations of several key terms: “authorized representative,” “directory information,” “early childhood education program,” and “education program.” In addition, in the preamble to the final regulations, the Department offers its views on the differences between “educational agency,” “educational institution,” and “state and local educational authority.”

“Authorized representative” is a new, defined term and represents a departure from the Department’s prior interpretation of FERPA. Under the new definition, an authorized representative is any entity or individual designated by a state or local educational authority, the Department of Education, the Department of Justice (“DOJ”), or the Government Accountability Office to conduct—with respect to federal or state-supported education programs—any audit or evaluation, or any compliance or enforcement activity in connection with federal legal requirements that relate to such programs.

Though not defined in the prior regulations, the words “authorized representative” had been interpreted by the Department prior to January 3, 2012, not to encompass other state or federal agencies (i.e. a state department of health and human services or state department of labor) because they were not under the direct control of state educational authorities, or control of agencies headed by the Secretary, Attorney General, or Comptroller General. Thus, a state department of education formerly could not make further disclosures of personally identifiable information from
education records to such departments without a student's consent.

Under the revised regulations, the Department could designate a much wider range of individuals or entities to be its authorized representatives. For example, it could designate a trade union to receive personally identifiable information to evaluate the effectiveness of a university in preparing students for the workplace. Similarly, a private researcher or nonprofit agency could be authorized to receive personally identifiable information to conduct an audit or evaluation of the Teacher Quality Partnership Grant Program authorized under Title II of the Higher Education Act.

To accompany this broader definition of “authorized representative,” the Department provided some safeguards. The personally identifiable information that is disclosed may be used only for the purpose indicated, and a written agreement with required terms must be used to designate the authorized representative. In addition, the designating authority or official is responsible for using reasonable methods to ensure that an authorized representative uses the information only for an authorized purpose, protects the information from further disclosures or uses it as indicated in the regulations, and destroys the personally identifiable information when no longer needed for the designated purpose. The information must be protected in a way that does not permit personal identification of individuals by anyone other than the state or local educational authority, the Department of Education, the Department of Justice, or the Government Accountability Office, and their authorized representatives.

“Directory information” is redefined and includes a new limitation placed upon a parent or eligible student's ability to opt-out of directory information. Under prior and current regulations, a parent or eligible student may not use the opt-out authority to prevent an educational agency or institution from disclosing or requiring a student to disclose the student's name, identifier, or institutional email address in a class in which the student is enrolled. The new regulations expand that list and explain that the right to opt-out also does not include the right to refuse to wear or otherwise disclose a student identification (ID) card or badge that contains identifying information (typically a name, photo, and student ID number). This new provision thus further limits a parent’s authority under the act “to inform the institution or agency that any or all of the information designated [as directory information] should not be released without the parent's [or eligible student’s] prior consent.

Institutions of higher education have generally welcomed the new limitation, as it provides a means of additional campus security and classroom management.

“Education program” is another new, defined term and encompasses any program that is principally engaged in the provision of education, including early childhood education (another newly defined term in the regulations), elementary and secondary education, postsecondary education, special education, job training, career and technical education, adult education, and any program that is administered by an educational agency or institution of higher education.

The breadth of this definition becomes important in the application of the audit and evaluation exception. Under that exception, a college or university may disclose personally identifiable information from education records, without consent, to authorized representatives in connection with an audit, evaluation, or enforcement of federal legal requirements related to federal or state-supported education programs. Thus, the potential range of education programs from which data may be shared for purposes of audits, evaluations, or compliance activities is quite broad—ranging from early childhood programs to job training.

Further, in the preamble, the Department takes the position that “education programs” are broad enough to include not only traditional academic programs, but also cyber-security, substance abuse, and violence prevention programs and the like, when administered by an educational agency or
C. Legal Authority to Audit or Evaluate Education Programs

For purposes of the non-consensual disclosure of personally identifiable information to authorized representatives, the legal authority to conduct an audit, evaluation, compliance or enforcement action need no longer be express, and may now simply be implied from other federal, state or local laws. This change is significant, in that previously, the legal authority to conduct an audit, evaluation, or compliance or enforcement activity had to be “established under other Federal, State, or local authority.” The deletion will make it easier for agencies and officials to go about audits, evaluations, and enforcement and compliance activities, but it also represents a major shift in FERPA law and policy, and some have questioned its legal basis.

As applied, a private institution of higher education can disclose (although it is not required to do so under federal law), without a student’s consent, personally identifiable information to a State Longitudinal Data System (“SLDS”) for the purpose of the SLDS’s audit of, for example, a reading program. It may be done without the SLDS establishing the express legal authority under another federal, state, or local law to conduct the audit. In other words, the administrator of the SLDS is not required to determine whether there is legal authority, and the authority will be implied from the administrator’s decision to proceed.

D. Expansion of Audit and Evaluation Exception to Include Recipient of Data

In a related vein, a prior Department interpretation allowing personally identifiable information to be used only for audits, evaluations, or compliance or enforcement activities of the disclosing agency’s education programs is expanded to allow use of the information with respect to the recipient’s education programs as well. For example, a college (disclosing agency) could disclose (though it is not required to do so under FERPA), without consent, personally identifiable information to a school district about the school district’s former students who are now in attendance at the college, for purposes of evaluating an education program of the school district (recipient agency).

E. Re-disclosure “On Behalf Of” Educational Agencies and Institutions Under the Audit and Evaluation Exception

The amended regulations permit a state or local educational authority, or the Department of Education, Department of Justice, or the Government Accountability Office to make further disclosures of personally identifiable information on behalf of the educational agency or institution of higher education from which it received the information even if the agency or institution of higher education objects. However, the re-disclosure must meet one of the several exceptions to consent, and the names of the parties to whom the disclosures are made must be recorded, as well as the legitimate interests of such parties.

To illustrate, a college could disclose personally identifiable information without consent to a state educational agency for purposes of an evaluation of a federal education dropout prevention program. The state educational agency may then re-disclose the personally identifiable information on behalf of the college to a local educational agency for an unrelated evaluation, even if the college objects, as long as it complies with the provisions noted above.

F. Re-disclosure “On Behalf Of” Educational Agencies and Institutions Under the Studies Exception

Similar to the audit and evaluation exception, the research studies exception is expanded to provide that a state or local educational authority, the Department of Education, Department of Justice, or
Government Accountability Office may enter into agreements with organizations conducting research studies and re-disclose personally identifiable information on behalf of educational agencies and institutions of higher education that initially provided the information, even if the agency or institution of higher education disagrees. The re-disclosure must be for a study designed to improve the institution’s instruction, or for any other purpose for which non-consensual disclosure of data is allowed. As with the audit and evaluation exceptions, the re-disclosure must meet one of the several exceptions to consent, and the names and legitimate interests of the parties to whom the disclosures are made must be recorded. An institution of higher education may request a copy of the record of further disclosures from the state or local educational authority, Department of Education, Department of Justice, or Government Accountability Office, and such copy must be provided within 30 days.

G. Enforcement

The enforcement provisions are also expanded in the amended regulations. The new regulations extend the reach of the Family Policy Compliance Office (“FPCO”) beyond educational agencies and institutions to student loan servicers, loan guaranty agencies, and lenders, under circumstances where education records are obtained from educational institutions. Because the FERPA statutory conditions only apply to an “educational agency or institution” at which students “are or have been in attendance at a school of such agency or at such institution,” extending the enforcement reach beyond educational agencies and institutions appears to reach beyond the scope of the statute.

For example, a complaint could be filed with FPCO against a student loan servicer, and FPCO could enforce FERPA against the servicer, even though the servicer is neither an educational agency or institution. The amended rules also consolidate into one section all provisions relating to the “five-year [disqualification] rule” for improper re-disclosures.

II. State Longitudinal Data Systems

As noted in the introduction, these new regulations and definitions are related largely to the fact that many states have authorized the creation of systems of student-based data known as State Longitudinal Data Systems (“SLDS”). These systems consist of data covering pre-kindergarten, K-12, postsecondary and postgraduate education, and workforce data commonly designated as a “P-20W” system. The data are used for purposes of accountability, program improvement, decision making, and informing public policy. Apart from state requirements or limitations, the new FERPA regulations make it easier for institutions of higher education to share data with a SLDS. While SLDS are generally populated with data from public institutions or agencies, some states require private institutions of higher education to disclose personally identifiable information to the SLDS. Others “authorize” the collection of data from non-public institutions of higher learning effectively making their participation permissive.

It is important to reiterate that FERPA does not grant authority to states or to the federal government to collect student data. Rather as noted earlier, the Act conditions the availability of federal education funds upon certain policies and practices of education agencies and institutions regarding the review and disclosure of records. For purposes of FERPA, an institution of higher education may disclose personally identifiable information from student education records without the consent of the student, provided one of several exceptions is met.

For example, if a state department of education oversees a SLDS and the longitudinal data system is used to audit or evaluate how well students transition academically to postsecondary education, an institution of higher education could share personally identifiable information with the SLDS without the consent of the students, assuming no inconsistency with state law. In a similar manner, if
a state commission or board manages a SLDS, a state department of education could designate the commission or board as its authorized representative to receive personally identifiable information from education records, provided the records are disclosed for the purpose of an audit or evaluation.

III. Data-Sharing Agreements

A. Checklist of Terms for State Longitudinal Data System Data-Sharing Agreement

With these new regulations and the increased use of data by federal, state, and local governments for decision making, colleges and universities can expect more requests for student education records. As an institution of higher education considers sharing personally identifiable information from student education records, such as for an SLDS, it should first determine whether the institution is required to do so under state law, or whether it is a discretionary matter. In either case, if personally identifiable information will be shared, a written agreement should set forth the terms and incorporate any terms that state law may require. The institution should also ensure that any sharing of personally identifiable information fits within one of the several exceptions to consent. [57]

Absent any specific terms required by state law, the following non-comprehensive list of terms should be considered for any SLDS agreement:

- Purpose, scope and duration of the agreement;
- Personally identifiable information from the education records of the institution must only be used for the purposes of the agreement;
- SLDS provides assurances that it will comply with FERPA and applicable laws;
- SLDS may grant access to personally identifiable information only to individuals with a need to know;
- SLDS shall take steps to maintain the confidentiality of the personally identifiable data at all stages;
- SLDS must destroy the personally identifiable information when the information is no longer needed;
- Specify the means to destroy the information;
- If the institution and SLDS reach an agreement to permit re-disclosure, the SLDS must affirmatively notify the institution of higher education no less than “X” days prior to the intended re-disclosure of the applicable FERPA exception, the additional party that will receive the data, and the legitimate interest of the additional party;
- How to amend and terminate the agreement;
- “Definitions” section that distinguishes “improper re-disclosure” from “data breach” and defines other relevant terms;
- Require the SLDS to submit a data security/stewardship plan that satisfies the institution prior to data-sharing;
- Recitals to state law on data breach;
- Specific data breach protocols to be followed in the event of a data breach with clarification of the means that will satisfy notice requirements (e.g. written notice, electronic notice, telephonic notice, web-based notice, etc.);
- To the extent consistent with state law, the SLDS will hold harmless and indemnify the institution of higher education for any damages, costs, or attorney’s fees incurred as a result of an investigation, claim or litigation resulting from a data breach, whether the breach is by the SLDS or a third party who receives personally identifiable information from the SLDS;
- Require periodic reports by the SLDS and third parties to the higher education institution;
- Right to audit, inspect, or monitor activities of the SLDS unannounced;
- Clarify ownership rights in the data;
- Statement of how disputes between the institution and the SLDS will be resolved;
• Points of contact and data custodians

B. Studies Exception Agreements

For institutions of higher education that desire to undertake a study for the purpose of developing, validating, or administering predictive tests, administering student aid programs, or improving instruction, and in doing so the institutions permit access to personally identifiable information without consent, the amended regulations require inclusion of the following four terms in a written agreement: [58]

• Specify the purpose, scope and duration of the study and the information to be disclosed;
• Specify that the personally identifiable information from the student education records of the institution must be used only for the study;
• Require the entity to conduct the study in a manner that does not identify students or their parents. This means the organization should allow internal access to the personally identifiable information from education records only to individuals with a need to know. The recipient organization should be required to take steps to maintain the confidentiality of the personally identifiable information from education records at all stages of the study, including the final report, by using appropriate disclosure avoidance techniques;
• Require the organization to destroy the personally identifiable information from education records when the information is no longer needed for the identified study. The institution of higher education should determine the specific time period for destruction based on the facts and circumstances surrounding the disclosure and study.

C. Audit and Evaluation Agreements

Similarly, in the event an institution of higher education agrees to serve as an authorized representative, [59] the institution will review, presumably, personally identifiable information from another entity (other than the institution of higher education) under the audit and evaluation exception. [60] Under the exception to consent, the review will be for purposes of any audit, evaluation, or compliance or enforcement activity in connection with federal legal requirements that relate to federal or state-supported education programs. Under the amended regulations, the institution should be aware that it will be required to sign a written agreement with the entity that designates it as an authorized representative. The agreement must include the following terms: [61]

• Designate the entity [institution of higher education] as the authorized representative;
• Specify the personally identifiable information from education records to be disclosed;
• Specify the purpose of disclosure to the authorized representative is for an audit or evaluation of federal or state-supported education programs, or to enforce or comply with federal legal requirements that relate to those programs;
• Provide a description of the activity with specificity to make clear the work falls within the exception to the student's written consent;
• Require the authorized representative to destroy the information when the information is no longer needed for the purpose;
• Specify the time period in which the information must be destroyed;
• Establish policies and procedures to protect the personally identifiable information from further disclosure (except back to the disclosing agency) and unauthorized use (includes limiting use to only authorized representatives with legitimate interests in the audit or evaluation, compliance, or enforcement of federal legal requirements related to these programs).

A more likely scenario is that the agreement will arise in the context of another entity designated as an authorized representative by a state or local educational authority, the Department of Education, Department of Justice or Government Accountability Office, and with such designation may receive
access to personally identifiable information from student education records of the institution (assuming the institution agrees to disclose). The institution should be aware that the authorized representative will be subject to the same terms as above. [62]

CONCLUSION:

What is the net result of the revised FERPA regulations? The result is greater freedom for state and local educational agencies, the Departments of Education and Justice, the Government Accountability Office, authorized representatives, and others to access personally identifiable information without consent, for purposes of evaluation, accountability, and fiscal stewardship. Some worry, however, that this increased freedom weakens the privacy protections surrounding student education records. Whatever one's view, requests for student information will become more prevalent and colleges and universities should ensure that when sharing personally identifiable student data, they have a written agreement that sets forth all required terms and privacy expectations.

ENDNOTES:


3. Id.


5. The words “without the consent of the student,” “without consent,” and “non-consensual” are used synonymously throughout. The words “student” and “students” are used throughout rather than “parent” or “parent and student.” Under FERPA, a student who either has attained eighteen (18) years of age or is attending an institution of postsecondary education at any age assumes the rights of a parent. 20 U.S.C. § 1232g(d); 34 C.F.R. § 99.3 (defining “eligible student”).

6. The words “prior rules” refer to regulations in effect prior to January 3, 2012, the effective date of the amended regulations. The prior regulations remain in effect unchanged except as indicated. The regulations are found at 34 C.F.R. §§ 99.1-.67.

7. Elec. Privacy Info. Ctr. (EPIC), et al., v. U.S. Dep’t of Education, No. 1:12-cv-00327(ABJ) (D.D.C. Feb. 29, 2012). On November 30, 2012, the Department filed a Motion to Dismiss or In the Alternative for Summary Judgment. EPIC’s Opposition and Cross Motion for Summary Judgment was filed January 19, 2013 and the Department’s Reply to EPIC on February 1. On February 15, 2013, EPIC filed a Reply in support of its Cross Motion. The Joint Appendix was filed March 1. No hearing date has been set as of the date of this Note.

8. The “audit and evaluation” exception refers to one of several exceptions to the requirement that consent be obtained from a parent or eligible student in order to disclose personally identifiable information from education records. 20 U.S.C. §§ 1232g(b)(1)(C), (b)(3), and (b)(5); 34 C.F.R. § 99.35. Specifically, this exception permits educational agencies and institutions to disclose personally identifiable information from education records, without consent, to authorized
representatives of state and local educational authorities, the Secretary of Education, the Attorney General of the United States, and the Comptroller General of the United States, as may be necessary in connection with the audit, evaluation, or the enforcement of federal legal requirements related to federal or state-supported education programs. Key to the exception is the expansiveness of the definition of “authorized representative” in the new rule. The definition establishes the scope of the exception. 34 C.F.R. § 99.3 (“Authorized representative means any entity or individual designated by a State or local educational authority or an agency headed by an official listed in § 99.31(a)(3) to conduct—with respect to Federal-or State-supported education programs—any audit or evaluation, or any compliance or enforcement activity in connection with Federal legal requirements that relate to these programs”). The “studies” exception permits educational agencies and institutions to disclose personally identifiable information from education records, without consent, to organizations conducting studies for, or on behalf of, educational agencies and institutions to improve instruction, to administer student aid programs, or to develop, validate, or administer predictive tests. 20 U.S.C. § 1232g(b)(1)(F); 34 C.F.R. § 99.31(a)(6). The new rule construes this exception expansively to permit re-disclosures of personally identifiable information on behalf of the educational agency or institution that initially provided the information, even if the agency or institution disagrees. 34 C.F.R. §§ 99.31(a)(6)(ii) and (iii), and 99.33(b).


11. Id.

12. 20 U.S.C. § 1232g(a) and (b).


17. Id.

18. 34 C.F.R. § 99.3.


20. 34 C.F.R. § 99.3 (defining “authorized representative”).


23. Id.


25. 34 C.F.R. § 99.35.


27. 34 C.F.R. § 99.35(b)(1).

28. 34 C.F.R. § 99.3 (defining “directory information” at (c)(2)).


30. 34 C.F.R. § 99.37(c)(1).

31. 34 C.F.R. § 99.3 (defining “directory information”); 34 C.F.R. § 99.37(c)(2).


33. 34 C.F.R. § 99.3 (defining “education program”).

34. 20 U.S.C. § 1232g(b)(1)(C), (b)(3), and (b)(5).


37. See pre-January 3, 2012 version of 34 C.F.R. § 99.35(a)(2) (“Authority for an agency or official listed in § 99.31(a)(3) to conduct an audit, evaluation, or compliance or enforcement activity is not conferred by the Act or this part and must be established under other Federal, State, or local authority.”); see also the amended version 34 C.F.R. § 99.35(a) which deletes the preceding text of § 99.35(a)(2).

38. A public institution of higher education may be obligated to disclose certain information to State Longitudinal Data Systems where federal grants have funded such systems. See 20 U.S.C. §§ 9607, 9871(c), (e); American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, § 14005(d)(3), 123 Stat. 115, 283 (2009).


41. 34 C.F.R. §§ 99.33(b) and 99.35(b)(1).

42. 34 C.F.R. §§ 99.31(a)(6)(ii) and (iii), and 99.33(b).

43. Id.

44. Id.

45. 34 C.F.R. § 99.32(b)(2)(iii).


49. See also 20 U.S.C. § 1232g(a)(1)(B) (right of parents to inspect and review education records applies to records “on their children who are or have been in attendance at any school of an educational agency or institution”); 20 U.S.C. § 1232g(a)(2) (Opportunity for a hearing to challenge the content of education records applies to parents of students “who are or have been in attendance at a school of such [educational] agency or at such institution”). Absent from the text of § 1232g(a) is any mention of a “third party[] outside the educational agency or institution” where students are not or have not been in attendance. See expansion of enforcement authority to third parties, 34 C.F.R. § 99.67(c).

50. The “five-year rule” requires an agency or institution of higher education to prohibit access of a third party to personally identifiable information for a period of not less than five years if the FPCO finds that the third party improperly re-disclosed FERPA-protected data that the third party earlier received under one of the exceptions to consent.

51. The scope of this Note does not analyze state longitudinal data system laws. Rather, it references a few state laws to illustrate how some states have addressed data-sharing. See MD. CODE ANN., EDUC. § 24-707 (LexisNexis 2012) (“For-profit and private nonprofit institutions of higher education shall transfer student-level enrollment data, degree data, and financial aid data for all Maryland residents to the Maryland Longitudinal Data System in accordance with the data security and safeguarding plan developed under § 24-704(g)(6) of this subtitle.”); MINN. STAT. § 136A.1701 SUBD. 11 (2011) (“(a) An eligible institution [under the Minn. Supplemental and Additional Loans Program] must provide to the [Minnesota Office of Higher Education] data on student enrollment and federal and state financial aid.”); accord MINN. STAT. 136A.121 SUBD. 18 (2011) (Minn. Grants Program).

52. 105 ILL. COMP. STAT. 13/20(c) (2012) (“Beginning on July 1, 2012, the Board of Higher Education is authorized to collect and maintain data from any non-public institution of higher learning enrolling one or more students receiving Monetary Award Program grants and any non-public institution of higher learning that confers graduate and professional degrees, pursuant to Section 35 of the Higher Education Student Assistance Act, and disclose this data to the longitudinal data system for the purposes set forth in this Act. Prior to July 1, 2012, any non-public institution of higher education may elect to participate in the longitudinal data system by disclosing data for one or more of the purposes set forth in the Act to the Board of Higher Education or to a consortium that has contracted with the Board of Higher Education pursuant to this subsection (c).”).

53. See MINN. STAT. § 136A.05 SUBD. 1 (2012) (“Private postsecondary institutions are requested to cooperate and provide information [requested by the Minnesota Office of Higher Education in order to enable it to carry out and perform its duties].”); MINN. STAT. § 136A.05 SUBD. 2 (2012) (“Private postsecondary institutions are requested to cooperate and provide data [to and as requested by the Minnesota House of Representatives or Senate for research projects and studies qualifying under Code of Federal Regulations, title 34, section 99.31(a)(6)][FERPA “studies exception”]. As a condition of receiving the data, the house of representatives [sic] or senate [sic] shall enter into an agreement with the office or institution to ensure that the house of representatives [sic] or senate [sic] will not disclose any data that identify individuals.”); 105 ILL. COMP. STAT. 13/20(c) (2012) (“The Board of Higher Education may contract with one or more voluntary consortium of non-public institutions of higher learning established for the purpose of data sharing, research, and analysis. The contract may allow the consortium to collect data from participating institutions on behalf of the Board of Higher Education.”) 105 ILL. COMP. STAT. 13/25(d) (2012) (“Data that has been submitted to the [Board of Higher Education] by a consortium of non-public colleges and universities is prohibited
from being included in any interstate data-sharing agreements with other states unless consortium participants agree to allow interstate data sharing. Any non-public college may prohibit its data from being shared with any other state. Any non-public college may prohibit its data from being included in any interstate data-sharing agreement.


55. See 20 U.S.C. § 1232g(a)-(b).

56. 20 U.S.C. § 1232g(b)(1).

57. Id.

58. 34 C.F.R. § 99.3(a)(6)(iii)(C).

59. See 20 U.S.C. §§ 1232g(b)(1)(C) and (b)(3), 34 C.F.R. § 99.35, 34 C.F.R. § 99.3 (defining "authorized representative").

60. 34 C.F.R. § 99.35.

61. 34 C.F.R. § 99.35(a)(3).

62. Id.

RESOURCES:

Final Regulations of December 2, 2011 (last visited February 1, 2013).


An Overview for Parents and Students (last visited February 1, 2013).

Guidance for Reasonable Methods and Written Agreements (last visited February 1, 2013).

See Model Notification for Postsecondary Officials at Family Policy Compliance Office (last visited February 1, 2013).


NACUA FERPA Resource Page

Higher Education Compliance Alliance Resource Page on Privacy and Student Records
"To advance the effective practice of higher education attorneys for the benefit of the colleges and universities they serve."