OHIO SCHOOL BOARDS ASSOCIATION CAPITAL CONFERENCE

SCHOOL LAW WORKSHOP

"Protecting Your Students and their Privacy"

Susan G. Clark, Ph.D., J.D.
Professor, University of Akron

Columbus, OH
November 15, 2011

I. Introduction

A. The collection, maintenance, and use of student data are necessary administrative functions.

1. Instruction

2. Operations

3. Management

4. Accountability

5. Research and Evaluation

B. Breaches of data security cause harm.

1. To the student, e.g., identity theft, discrimination, emotional distress.

2. To the school district, e.g., financial loss, loss of public confidence and public reputation, and administrative burdens in investigating the breach and ensuring remedial steps are taken.

C. Educators shall comply with state and federal laws related to maintaining confidential information or risk a finding of "conduct unbecoming" to the profession.

1. Adopted March 11, 2008, by the State Board of Education, the Licensure Code of Professional Conduct for Ohio Educators applies to all individuals licensed by the Ohio Department of Education. Principle 5 addresses confidentiality.

"An educator is entrusted with information that could be misused to embarrass or damage a student's reputation or relationship with others. Therefore, the educator has the responsibility to keep information about students confidential unless disclosure serves professional purposes, affects the health, safety, and welfare of students and others, is required by law, or parental permission has been given. An educator maintains the security of confidential information such as academic and disciplinary records, personal confidences, photographs, health and medical information, family status and/or income." (Licensure Code, p. 8).

2. Conduct unbecoming to the profession includes, but is not limited to:

a. Willfully or knowingly violating any student confidentiality required by federal or state laws, including publishing, providing access to, or altering confidential student information on district or public websites such as grades, personal information, photographs, disciplinary actions, or individual educational plans ("IEPs") without parental consent or consent of students 18 years of age and older.

b. Using confidential student, family, or school-related information in a non-professional way (e.g., gossip, malicious talk or disparagement).

3. The appropriate range of disciplinary action for a violation of Principle 5 is suspension (1 day to 2 years) of a license. (Licensure Code, p. 16).

Caveat/Practice Pointer - O.R.C. §§3319.313 requires public and nonpublic schools, and community schools to report to the state superintendent, the name and a factual statement of any license holder who engages in conduct unbecoming to the teaching profession.

II. Students Have a Constitutional Right to Privacy

L.S. v . Mount Olive Bd. of Educ., 2011 WL 677490 (D.N.J., Feb. 25, 2011). A federal district court held that a social worker and special education teacher employed by the school board were liable for negligence and for violating a high school student's ("S.S.") federal and state

constitutional right to privacy for intentional disclosure of the student's confidential psychiatric evaluation to a class of 11th graders. As part of a class assignment, students were instructed to prepare a psychological or psychiatric evaluation on Holden Caulfield, the protagonist in the novel, The Catcher in the Rye. The special educator asked the social worker for a sample evaluation to distribute to the class and was given S.S.'s report, from which he made a redacted copy for distribution. A student in the class deduced that the report was about S.S. and told S.S.'s parents. The parents informed the high school administration, who promptly collected and destroyed all copies of the evaluation. The parents filed a complaint alleging causes of action under 42 U.S.C. §1983 for violation of S.S.'s constitutional right to privacy under the Fourth and Fourteenth Amendments, and his rights under the First Amendment, as well as state constitutional claims, statutory violations including IDEA and FERPA, and general negligence.

The parents claimed that school officials owed a duty to ensure the confidentiality of student records and breached this duty by failing to adequately educate and train school staff in the importance and implementation of the board's privacy policy, thereby causing the disclosure of S.S.'s psychiatric evaluation. The Third Circuit held that liability could not be predicated solely based on a theory of respondeat superior because individual defendants in a civil rights action must have personal involvement in the alleged wrongs and dismissed all claims against the superintendent, principal, and director of special services. The court also dismissed the §1983 claim against the school board for violation of S.S.'s right to privacy as no evidence was presented of the board's "deliberate indifference" with regard to maintenance of records or to personnel training. As for the social worker and special educator, the court found that S.S. had a constitutionally protected right to privacy in his psychiatric evaluation under the Fourteenth Amendment Due Process Clause and that the intentional disclosure of the student's records violated that right. The court let the negligence claims against the special educator and social worker stand as "no reasonable juror could find that they did not breach their duty to maintain the confidentiality of S.S.'s student records." FERPA and IDEA claims were dismissed because they provide no cause of action for damages.

Caveat/Practice Pointer - Under Section 1983, school officials can be held liable for a violation of a student's constitutional right to privacy if they have actual knowledge of breaches of confidentiality, direct disclosures, or acquiesce to such disclosures. A school board may be found liable under Section 1983 if the violation occurred as a result of established policy or custom. If the policy does not facially violate the law, the board could still be liable if its action was done with deliberate indifference as to its known or obvious consequences. A board also can be liable under Section 1983 if it fails to supervise or train its employees or personnel, if such failure exhibits a "deliberate indifference to the rights of persons" with which they come into contact. To protect against exposure, ensure that policies protect student rights to privacy, that school officials know and implement the policies, and that actions are taken to mitigate breaches and prevent further breaches.

III. Family Education Rights and Privacy Act ("FERPA"); 20 U.S.C. § 1232g; 34 C.F.R. Part 99.

A. FERPA is a federal law which protects the privacy of education records in all public elementary and secondary schools, school districts, state education agencies, and any public or private agency or institution that receives federal funding from the U.S. Department of Education ("USDOE").

1. The USDOE issued a notice of proposed rulemaking April 8, 2011 regarding FERPA. The public commentary period closed May 23, 2011. The final regulations are expected soon. Revisions were necessary because the American Recovery and Reinvestment Act of 2009 ("ARRA"), required states to adopt statewide longitudinal data systems ("SLDS") as a condition of funding, and further specifies the elements to be included. (76 Fed. Reg. 19726-19727). In relevant part, proposed changes are identified in this outline.

2. O.R.C. §3319.321, Ohio's Records Access and Confidentiality Law generally aligns with FERPA. Key differences are identified in this outline.

3. OAC 3301-51-04, Ohio's Special Education Confidentiality Rule generally aligns with FERPA, 20 U.S.C. §1415; 34 C.F.R §300.121. Key differences are identified in this outline.

B. The USDOE Family Policy Compliance Office ("FPCO") enforces FERPA and provides technical assistance to schools to ensure compliance with FERPA and its regulations. 34 C.F.R. Part 99, Subpart E.

1. Gonzaga Univ. v. Doe, 536 U.S. 273 (2002). The U.S. Supreme Court held that there is no private right of action to sue for a violation of FERPA.
2. Letter to Anonymous, 109 LRP 25325 (FPCO, 2009). The FPCO concluded that the school district violated FERPA and directed it to provide written assurance that steps were taken to protect against future improper disclosures. In this case, the parents wanted additional remedies including public sanction, loss of federal stimulus monies, etc., but the FPCO stated that the parents' proposed remedies were beyond FERPA's scope.

3. FERPA violations may result in a withholding or loss of federal funds. 20 U.S.C. §1232g(f); 20 U.S.C. §12334; 34 C.F.R. §90.67.

Caveat/Practice Pointer - The proposed FERPA regulations provide that state educational authorities and other recipients of funds from USDOE – not just educational agencies or institutions that enroll students – are subject to investigations and enforcement, including possible withholding of funds, for FERPA violations. This change is recommended because proposed regulations also expand the definition of "education programs" that may be the subject of an evaluation or audit as the basis for disclosures under FERPA. The definition includes any program principally engaged in education, including, but not limited to, early childhood education, postsecondary education, career and technical education, adult education, and job training, whether or not the program is administered by an educational agency or institution.

C. FERPA limits the scope of access to personally identifiable information contained in education records.[1]

1. "Education records" are records that contain information that are directly related to a student; and are maintained by an educational agency or by a party acting for the agency.

a. Records of law enforcement officers that are created for a law enforcement purpose by a law enforcement unit and maintained by the law enforcement unit are not education records.

Caveat/Practice Pointer - Law enforcement unit officials who are employed by the school may be designated "school officials." As such, they may be given access to personally identifiable information from students' education records. The school's law enforcement unit officials must protect the privacy of education records it receives and may disclose them only in compliance with FERPA. For that reason, FPCO advises that law enforcement unit records be maintained separately from education records. Letter to Bresler (FPCO, February 15, 2006).

[1] Parents and eligible students have additional rights under FERPA, 34 C.F.R. Part 99, Subpart B including a) the right to inspect and review education records within 45 days of making the request; b) the right to copies of their child's education record at a reasonable copying fee but only if failure to provide them with a copy will prevents them from inspection and review; c) the right to seek to amend inaccurate or misleading content or content which invades the privacy rights of the child; d) the right to be informed of rights, of the right to a hearing, and to file complaints with the USDOE. In Ohio, these rights, as well as the rights under the IDEA for students served under the IDEA, transfer to the student upon reaching age 18 or when the student enters a postsecondary institution at any age ("eligible student"). 34 C.F.R. §99.5(a)(1). However, the school district must provide notice of that transfer under OAC 3301-51-05 to the student and the parents. OAC 3301-51-04 requires the adoption and implementation of written policies and procedures, approved by ODE, to ensure parents of students with disabilities have an opportunity to examine education records and to ensure protection of the confidentiality of personally identifiable information in regard to the collection, use, storage, disclosure, retention, and destruction of that information.

2. A "record" is "any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche."

   a. Information acquired through personal knowledge and observation is not governed by FERPA, as it does not meet the definition of a "record."

   b. A personal record is not an "education record" if kept in the maker's sole possession; used only as a personal memory aid; and is not accessible or revealed to anyone except a temporary substitute for record maker.

   c. E-mails generally are not education records unless they are maintained in the student's file.

      S.A. v. Tulare County Office of Educ., 2009 WL 3126322 (E.D. Cal. 2009). The parents of a student with autism requested copies of all emails concerning their child. They were given hard copies of emails that were printed and stored in the student's file, but no emails that had been deleted or may have been on the server. Unsuccessful at the state level, the parents filed suit in federal court on the ground that they were denied all emails about their child and that student records had been destroyed without notice. The court held that under FERPA's definition of an "education record," only the email messages that were "printed and placed" in the student's permanent file were "maintained" because nothing in FERPA "requires an LEA to maintain an email or any other record based solely on the fact that it contains personally identifiable information about a student." The court noted that the U.S. Supreme Court held that the word "maintain," as used in FERPA, "suggests FERPA records will be kept in a filing cabinet in a records room at the school or on a permanent secure database." (Owasso Indep. Sch. Dist. v. Falvo, 534 U.S. 426, 432-33 (2002).) The court found that deleted emails were not "maintained" by the district, even if they were kept in staff email in-boxes or could be electronically retrieved from the district's server, and thus, did not have to be produced.

Caveat/Practice Pointer - FERPA does not require training. However, OAC 3301-51-04(N)(3) requires that all persons collecting or using personally identifiable information on students with disabilities must receive training or instruction regarding FERPA policies and procedures. Neither does FERPA require that a person be appointed the custodian of student records, however such a person is implied. 34 C.F.R. §99.32(c)(2) provides that inspection of a student's education records is available to a "school official or his or her assistants who are responsible for the custody of the records." The Owasso Court opined, "FERPA implies that education records are institutional records kept by a single central custodian, such as a registrar[.]" (534 U.S. at 433-45). OAC 3301-51-04(N)(2), Ohio's special education law, requires that "one official at each participating agency must assume responsibility for ensuring the confidentiality of any personally identifiable information." Finally, OAC 3301-51-04(O) requires that parents must be informed when personally identifiable information collected, maintained, or used is no longer needed to provide educational services to the child and must destroy the information at the parent's request. There is no comparable FERPA requirement, except a record cannot be destroyed when an outstanding request is made to inspect and review a record. 34 C.F.R. §99.10(e). A permanent record of a student's name, address, telephone number, grades, attendance record, classes attended, grade level completed, and year completed shall be maintained without time limitation.

d. Video surveillance generally does not meet the definition of an education record because it records everything and is not directly related to any student. There is no official guidance from FPCO on the matter of video surveillance.

Caveat/Practice Pointer - If video surveillance captures a student committing misconduct in violation of school rules, e.g., breaking into a locker, only that portion of the video may become part of that student's education record if the video is used as evidence for discipline. If more than one student is involved in an incident, e.g., a fight, a surveillance video may become the education record of each student involved in the altercation if the video will be used for disciplinary purposes. Under FERPA, when a video is an education record of more than one student, each parent must provide written consent before the video can be inspected by the other parent. 34 C.F.R. §99.12(a). Regarding students with disabilities, OAC 3301-51-04(F) provides that if any education record includes information on more than one child, the parents of those children have the right to inspect and review only the information relating to their child or to be informed of that specific information. Finally, a video is not the education record of students who are merely present when the misconduct occurs unless the video is used to find witnesses and the student is named or used as a witness. Treat as you would a witness statement.

D. FERPA requires written parents/eligible student consent before disclosing personally

identifiable information contained in education records, unless the disclosure is an authorized exception to this consent requirement.

Caveat/Practice Pointer - Written consent must be signed and dated by the parent/eligible student before disclosure can be made and must a) specify the records that may be disclosed; b) state the purpose of the disclosure; and c) identify the party or class of parties to whom the disclosure may be made. Written consent may be electronic if the district authenticates that the particular person is the source of the consent. 34 C.F.R. §99.30.

1. "Disclosure" means to permit access to, or the release, transfer, or other communication of, personally identifiable information contained in education records to any party, by any means, including oral, written, or electronic means.

2. "Personally identifiable information" includes, but is not limited to:

    a. The student's name, or the names of the student's parents or other family members;

    b. Personal identifiers, e.g., the student's social security number, ID number, or biometric record (e.g., DNA, handwriting); or indirect identifiers, e.g., the student's date or place of birth, or mother's maiden name;

    c. 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;

    d. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education records relates.

3. Disclosure without written parental/eligible student consent is permitted under certain circumstances and conditions. The Preamble to FERPA regulations, 73 Fed. Reg. 74814 (Dec. 9, 2008) state that disclosure under any of the conditions below is discretionary. 34 C.F.R. §99.31.

    a. To an eligible student (over age 18) or to parents of an eligible student where the student is a dependent as defined by IRS tax rule 152.

        (1) In the case of divorce or separation, each parent, residential or nonresidential, retains FERPA rights subject to any statute, court

order, or legally binding agreement governing the rights of such parents. 34 C.F.R. §99.4.

b. The information is designated by school board policy as "directory information" and notice of what constitutes directory information is provided in the district's annual notification.

(1) "Directory information" is information contained in a student's education record that would not generally be considered harmful or an invasion of privacy if disclosed, e.g., the student's name, email address, participation in officially recognized activities and sports, weight and height of athletes, honors and awards received, student ID numbers, user IDs, or other unique personal identifier used by the student for purposes of accessing or communicating in electronic systems, but only if the identifier cannot be used to gain access to education records except when used in conjunction with other methods of identity authentication.

Caveat/Practice Pointer - The proposed changes to the FERPA regulations will permit school districts to limit the disclosure of directory information to specific parties, for specific purposes, or both, after providing public notice. O.R.C. §3319.321(A) specifically prohibits the release of, or access to directory information to any person or group for use in a profit-making plan or activity and permits school authorities to request disclosure of the requestor's identity or the intended use of the directory information so as to ascertain whether the directory information is for use in prohibited activities.

(2) Annual public notice must inform parents/eligible students of the types of personally identifiable information that will be designated directory information and the time frame in which they may provide written notice of their choice to "opt out" of such disclosure without consent. 34 C.F.R. §99.37.

(a) A provision of the No Child Left Behind ("NCLB") Act, Section 9528, requires the release of secondary students' names, addresses and telephone numbers to military recruiters who request them unless parents have "opted out" of such disclosure. 20 U.S.C. §7908.

Caveat/Practice Pointer - A school district may disclose directory information about former students, however, if the students previously "opted out"of such disclosures, the school district must continue to honor that request, unless the student rescinds it. Regulations prohibit parents/eligible students in attendance from opting out from directory disclosures to prevent the school from disclosing or requiring the student to disclose his/her name, identifier, or institutional email address. 34 C.F.R. §99.37. The proposed FERPA regulations provides that parents may not opt out of directory information disclosures to prevent the school from requiring students to wear or otherwise disclose student ID cards or badges when on school property or engaged in school events.

c. To "school officials" deemed to have a "legitimate educational interest" as defined in the school district's required annual notification of FERPA rights.[2]

(1) "Legitimate educational interest" may be defined as a need to review education records so as to fulfill professional duties.

(2) "School officials" may be defined as teachers, bus drivers, attorneys, board members, and may include contracted third parties such as consultants, volunteers, or others to whom the district has outsourced work provided that the outside party:

(a) Performs an institutional service or function for which the school would otherwise use employees;

(b) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and

(c) Is subject to the requirements of §99.33(a) governing the use and redisclosure of information contained in education records.

[2] For a model notification, see, http://www2.ed.gov/policy/gen/guid/fpco/ferpa/lea-officials.html.

Caveat/Practice Pointer - To ensure that school officials obtain access to only those education records in which they have legitimate educational interests, the education agency must use "reasonable methods" to control such access, i.e., identify and authenticate the identities of those to whom the school discloses information. In the absence of electronic access controls, administrative policy should control. Currently, the regulations do not define the term, "reasonable methods," but the proposed regulation solicits public comment on what would constitute reasonable methods.

d. To student financial aid officials if the information is necessary for the determination of eligibility, amount, conditions, or enforcement of the terms and conditions of the aid.

e. To state and local officials in connection with serving the student under the juvenile justice system as established by state law, e.g., probation.

Caveat/Practice Pointer - O.R.C. §3319.321(E) permits disclosure without consent to a law enforcement officer who is conducting an investigation that the student is or may be a missing child. In that case, free copies of information in the student's record shall be provided, upon request, to the law enforcement officer, if prior approval is given by the student's parent, guardian, or legal custodian. Additionally, under O.R.C. §3319.321(H), to the extent allowable by FERPA, a principal is not required to obtain the consent of the pupil or the pupil's parent/guardian before making a report pursuant to O.R.C. §3319.45 that a pupil committed a violation listed in O.R.C. §3313.662(A) on property owned or controlled by, or at an activity held under the auspices of, the board of education, regardless of whether the pupil was sixteen years of age or older. Finally, school officials are not prohibited by IDEA from reporting crimes committed by a child with a disability to appropriate authorities. Upon reporting such a crime, copies of the special education and disciplinary records of the child shall be transmitted for consideration by the appropriate authorities to whom the agency reports the crime, to the extent that the transmission is permitted by FERPA. OAC 3301-51-04(R)(2).

f. To officials of schools to which a student intends to, or seeks to enroll or where the student is already enrolled, so long as the disclosure relates to the enrollment or transfer.

Caveat/Practice Pointer - OAC 3301-51-04(M)(2)(b) provides that if a child with a disability is enrolled, or is going to enroll in a nonpublic school that is not located in the school district of the parent's residence, parental consent must be obtained before any personally identifiable information about the child is released between officials in the school district where the nonpublic school is located and officials in the school district of the parent's residence. For students with disabilities who are parentally placed in nonpublic schools, OAC 3301-51-08(B)(8) provides that the school district where the chartered or non-chartered nonpublic school is located must adhere to all IDEA and FERPA confidentiality requirements when conducting child find, evaluation and service activities for parentally placed nonpublic school children with disabilities.

(1) Parental/eligible student consent must be obtained before the personally identifiable information of a student with a disability is released to officials of participating agencies providing or paying for transition services. OAC 3301-51-04(M)(2)(a).

(2) With regard to the transfer of records containing disciplinary information, OAC 3301-51-04(Q) provides that the records of a student with disabilities shall include a statement of any current or previous disciplinary action that has been taken against the child and transmit the statement to the same extent that the disciplinary information is included in, and transmitted with, the student records of nondisabled children.[3]

g. By judicial order or lawfully issued subpoena (reasonable efforts must be made to notify the parent of the intended disclosure).

h. In the event of a health or safety emergency where knowledge of the personally identifiable information is necessary to protect the health or safety of the student or other individuals.[4]

[3] The required statement must specify the circumstances that resulted in the disciplinary action and provide a description of the disciplinary action taken if the disciplinary action was taken because the child a) carried a weapon to or possessed a weapon at school, on school premises, or to or at a school function under the jurisdiction of a school district, county board of MR/DD, and other educational agency; b) knowingly possessed or used illegal drugs, or sold or solicited the sale of a controlled substance, while at school, on school premises, or at a school function under the jurisdiction of a school district, county board of MR/DD, and other educational agency; or c) inflicted serious bodily injury upon another person while at school, on school premises, or at a school function under the jurisdiction of a school district, county board of MR/DD, and other educational agency. The statement must also include any information that is relevant to the safety of the child and other individuals involved with the child; and may include a description of any other behavior engaged in by the child that required disciplinary action, and a description of the disciplinary action taken.

[4] There must be an articulable and significant threat to the health or safety of a student or other individuals, which must be recorded. The names of the parties to whom the institution disclosed the information must be recorded.

i. When a registered juvenile sex offender is enrolled or attending school and the school has notice under 42 U.S.C. §14071. [See Letter to Kansas School District re: Disclosure of Information About Juvenile Registered Sex Offenders (OCR, March 8, 2005)].

j. To organizations, e.g., federal, state, local agencies, and independent organizations, conducting studies for, or on behalf of, educational agencies or institutions to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction.

Caveat/Practice Pointer - Even where a school district's annual notification identifies specific contractors as "school officials," written agreements must be entered into between the board and the receiving organization that a) specify the purpose, scope and duration of the study/studies and the information to be disclosed; b) require the organization to use information only to meet the purpose of the study; c) require the organization to conduct the study in a manner that does not permit personally identifiable information of parents and students by anyone other than organization representatives with legitimate interests; d) require the organization to destroy or return all personally identifiable information when no longer needed for purposes of the study; and e) specify the time period in which the information must be returned or destroyed. If the FPCO finds that the third party organization did not destroy the information, it may disallow that party from access for at least five years (called "debarment").

k. To accrediting organizations in order to carry out their accrediting functions.

l. To authorized federal or state authorities conducting an audit, evaluation, or enforcement of education programs.

Caveat/Practice Pointer - The proposed regulations to FERPA provide that if an authorized representative that receives data to perform evaluations, audits or compliance activities is found by USDOE to have improperly redisclosed the data in violation of FERPA, the educational authority that provided the data would be required to deny access to personally identifiable data to that representative for at least 5 years.

m. For data reporting, such as SLDS collection mechanisms.

> **Caveat/Practice Pointer** - One of the key purposes of the proposed changes to the FERPA regulations is to substantially increase the number of entities permitted to access student data without parental or eligible student consent by expanding current exceptions for research, evaluation, audit, and accountability purposes, including enforcing federal compliance with state or federal supported education programs.

IV. Ohio's Education Repository System/Statewide Longitudinal Data System[5]

A. Effective December 28, 2010, O.R.C. §3301.94 permits the state superintendent of public instruction and the chancellor of the Ohio board of regents to enter into a memorandum of understanding under which the ODE, on behalf of the chancellor, will receive and maintain copies of data records containing student information reported to the chancellor for the purpose of combining those records with the data reported to the education management information system ("EMIS").

1. The purpose of this data sharing is to establish an education data repository that may be used to conduct longitudinal research and evaluation.

2. All costs related to the establishment and ongoing maintenance of the repository is to be paid from funds received from grants awarded under the ARRA, Title XIV, section 14006(a), other federal grant programs, or existing appropriations of the ODE or chancellor.

B. An independent contractor engaged by ODE would create and maintain student data verification codes and remove from the data record any information that would enable the code to be matched to personally identifiable student data. Data in the repository shall be managed in compliance with FERPA.

[5] OAC 3301-2-17 provides that the following federal statutes or regulations or state statutes and administrative rules make personal information maintained by the ODE confidential: social security numbers, 5 U.S.C. 552a; student education records, 20 U.S.C. 1232g {FERPA); student information in EMIS, O.R.C. §§3301.0714; 3319.321 ("confidentiality"); student test scores and information on Ohio achievement tests, O.R.C. §3301.0711(I); student data verification codes in combination with student name or other personally identifiable information, O.R.C. §§3310.42(D) (autism scholarship program); 3313.978(F) and 3310.11(D) (education choice pilot project scholarship program), and 3317.20(G) (payment to DD board).

Caveat/Practice Pointer - The proposed changes to the FERPA regulations require that state and local education authorities use "reasonable methods" to ensure compliance with FERPA by any entity designated as its authorized representative to receive data to conduct evaluations, audits, or compliance activities. Additionally, the proposed regulations authorize education agencies to store data in a state or local data agency that is not itself an education agency. Currently, the noneducation data have to be transmitted to the education agency and matched under its supervision.

C. Permitted uses of the data include, but are not limited to, audit and evaluation functions concerning higher education or concerning preschool, elementary, and secondary education as required or authorized by any provision of law.

Caveat/Practice Pointer - The proposed changes to the FERPA regulations authorize postsecondary institutions or data systems to disclose student data back to K-12 data systems or to school districts for the purpose of evaluating how well the district prepared students for college. The proposed regulations also permit K-12 agencies or data systems to disclose data back to publicly funded early childhood education programs to determine how well the programs prepared children for elementary school. Currently, the Preamble to 2008 regulations state that data may be disclosed under the evaluation/audit provision in FERPA only for the purpose of evaluating/auditing programs of the agency disclosing the data. Additionally, changes are proposed that are intended to remove barriers to linking education records with records maintained for pre-school, health and human services, labor, etc. This type of information-sharing would be provided under written agreements. Currently under FERPA, data may be disclosed only to employees or private contractors of education agencies, not to workforce or other state or local non-education agencies.

D. Written agreements may be entered into with entities contracted to conduct research and analysis to evaluate the effectiveness of programs or services, to measure progress against specific strategic planning goals, or for any other purpose permitted by law that the superintendent and chancellor consider necessary for the performance of their duties. These agreements may permit the disclosure of personally identifiable student information, provided that disclosure complies with FERPA.

Caveat/Practice Pointer - The proposed regulations also require written agreements between the state or local education authority and its authorized representative for evaluations, audits, and compliance activities that include a) the purpose and scope of the disclosures, b) the return or destruction of the data when no longer needed for the authorized purpose and the time period for such return or destruction, and c) policies and procedures to protect the data from misuse or further disclosure. The proposed regulations provide that nothing in FERPA prevents a state or local education authority from redisclosing data on behalf of educational agencies or institutions for a research study subject to an agreement with the research organization protecting use of data.

V. Protection of Pupil Rights Amendment ("PPRA"), 20 U.S.C. § 1232h(b) and (c); 34 C.F.R. Part 98 (as amended 2002).

A. The PPRA, and its amendments pursuant to NCLB Section 106, requires federal recipient education programs to have policies in place to protect the rights of parents and minor students. It seeks:

1. To ensure that schools and contractors make instructional materials available for inspection by parents if those materials will be used in connection with a USDOE funded survey, analysis, or evaluation in which their children participate; and
2. To ensure that schools and contractors obtain written parental consent before minor students are required to participate in any USDOE funded survey or any third party survey, analysis, or evaluation that reveals information concerning sensitive topics.[6]

B. Schools are required to develop and adopt policies in conjunction with parents regarding the following:

1. The right of parents to inspect, upon request, a survey created by a third party before the survey is administered or distributed by a school to students and arrangements to protect student privacy in the event the survey contains one or more of the same eight items of information footnoted below.

2. The right of parents to inspect, upon request, any instructional material used as part of the educational curriculum for students.

[6] Political affiliations; mental and psychological problems potentially embarrassing to the student and his/her family; sex behavior and attitudes; illegal, anti-social, self-incriminating and demeaning behavior; critical appraisals of other individuals with whom respondents have close family relationships; legally recognized privileged or analogous relationships, such as those of lawyers, physicians, and ministers; or income (other than that required by law to determine eligibility for participation in a program or for receiving financial assistance under such program). Religious practices, affiliations, or beliefs were added to the list by NCLB. 20 U.S.C. §1232(c).

3. The administration of physical examinations or screenings that the school may administer to students.

4. The collection, disclosure, or use of personal information collected from students for the purpose of marketing or selling, or otherwise providing the information to others for that purpose; and the right of parents to inspect upon request any instrument used to collect such information.

C. NCLB, Section 1061 the PPRA requires school districts to "directly" notify parents of these aforementioned policies at least annually at the beginning of the school year.

1. Parents must be notified of the specific or approximate dates during the school year when these activities are scheduled and must also be notified within a reasonable period of time if any substantive change is made to the policies.

2. In the notification, parent must be offered an opportunity for parents to opt out of a) any third party (i.e., non-USDOE funded) survey containing one or more of the above described eight items of information; and b) any nonemergency, invasive physical examination or screening that is required as a condition of attendance; administered by the school and scheduled by the school in advance; and not necessary to protect the immediate health and safety of the student, or of other students.

Caveat/Practice Pointer - Importantly, NCLB provides a number of exceptions to the opt out provision. The surveys exempted from opt out include the following subjects: college or other postsecondary education recruitment; military recruitment; book clubs, magazines and programs providing access to low-cost literary products; tests and assessments used to provide cognitive, evaluative, diagnostic, clinical, aptitude, or achievement information about students and the subsequent analysis and public release of the aggregate data from them; and the sale of products or services to raise funds for school-related or education-related activities; and student recognition programs. 20 U.S.C. §1232h(c)(4).

VI. Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §1320(d); 34 C.F.R. Parts 160 and 164.

A. The purpose of HIPAA is to standardize the electronic data interchange of health care transactions and to protect the privacy and security of personally identifiable health care information. The law contains of a number of rules.

B. The Privacy Rule establishes privacy requirements for oral, written or electronic individually identifiable health care information.

1. Where an outside party provides services directly to students, such as a public health nurse who provides immunizations, and is not employed by, under contract to, or otherwise acting on behalf of the school, these records would not be education records under FERPA, but would be records of a health care provider.

    a. With regard to these records maintained by a health care provider, the HIPAA Privacy Rule would apply only if the provider conducted one or more of the HIPAA transactions electronically, e.g., billing a health care plan for the services.

Caveat/Practice Pointer - School nurses who are under contract with, are employees of, or are otherwise under the direct control of the school, create and maintain student health records. Student health, medical, and immunization records maintained by a school district are, by definition, education records under FERPA. FERPA records are expressly excluded from coverage under the HIPAA Privacy Rule. (Preamble to the HIPAA regulation). These nurses/contractors may be identified as school officials under FERPA and written parental consent is required before school officials may disclose student health information unless a FERPA exception applies. Verification of a record is not a prohibited disclosure. FERPA permits school officials to contact the stated source of a record (such as a doctor's note regarding an excused absence) for verification purposes.

C. The HIPAA Transaction Rule may apply to school officials, e.g., school nurses, if education records are electronically transferred directly to the Ohio Department of Jobs and Family Services ("ODJFS") for purposes of Medicaid billing if the school district meets the criteria to be an Electronic Data Interface trading partner.

D. Ohio Medicaid School Program ("MSP")

1. Program documentation, treatment plans, eligible IDEA Part B services and IEP medically-related information maintained by school district employees and their contractors are FERPA protected and not covered by the HIPAA Privacy Rule. See, Letter to Mr. Dann Stevens, Iowa Dep't of Educ. (FPCO, October 12, 2005).

2. Under FERPA, schools may disclose education records if a parent has provided prior written consent to a third party authorized to receive the records, such as the designated Medicaid fiscal agent. 34 C.F.R. §99.30(a).

    a. Written parental consent must be obtained "each time" that a school district or other public agency seeks access to public benefits or insurance. 34 C.F.R. §300.154(d)(2)(iv)(A), (B).

b. "Each time" means that consent "may be obtained one time for the specific services and duration of services identified in a child's IEP." If the district later seeks to use public insurance to pay for additional hours of service (e.g., due to the IEP being revised or extended, it must seek parental consent again. See, Letter to John Hill, National Alliance for Medicaid in Education, Inc. (OSEP, March 8, 2007).

(1) As long as the period of consent does not exceed 365 days, a school district is permitted to ask for parental consent to cover a specific time period.

(2) A district does not need to seek parental consent if consent is given directly to another agency, such as the State Medicaid Agency, as long as the parental consent provided to the other agency meets the requirements set forth above. See, *id*., Letter to John Hill; Memorandum to State Directors of Special Education (OSEP, May 3, 2007).

Caveat/Practice Pointer - Consent for purposes of IDEA means that a) the parent has been fully informed of all information relevant to the activity for which consent is sought, in his or her native language, or other mode of communication; b) the parent understands and agrees in writing to the carrying out of the activity for which his or her consent is sought, and the consent describes that activity and lists the records (if any) that will be released and to whom; and c) the parent understands that the granting of consent is voluntary on the part of the parent and may be revoked at anytime. If a parent revokes consent, that revocation is not retroactive (i.e., it does not negate an action that has occurred after the consent was given and before the consent was revoked). 34 C.F.R. §300.9. Parents must be notified that refusal to allow access to their public benefits or insurance does not relieve the district or public agency of its responsibility to ensure that all required services are provided at no cost to the parents. In the event a parent refuses parental consent, it is recommended that the school district maintain documentation required by MSP standards, so that it can later bill MSP if the parents change their minds.

VII. National School Meals Programs

A. Federal law requires states and local education agencies to cooperate with Department of Agriculture studies and evaluations of the National School Lunch Act ("NSLA"), the Special Milk Program for Children; the School Breakfast program; the Summer Food Service Program; the Child and Adult Care Food Program, and more. (42 U.S.C. 1751; 7 C.F.R. Parts 210, 215, 220, 225, 226.

B. The confidentiality restrictions imposed by the school meals programs and milk program are more restrictive than FERPA. They are for the purpose of limiting the disclosure of a child's eligibility information and eligibility status to those who have a "need to know" for proper administration and enforcement of a federal education program.

1. Disclosure is defined as a child's program eligibility information obtained through the free and reduced price meal or free milk eligibility process that is revealed or used for a purpose other than for the purpose for which the information was obtained. The term refers to access, release, or transfer of personal data about children by means of print, tape, microform, microfiche, electronic communication or any other means. 7 C.F.R. § 245.1(a-3).

C. School district officials who are responsible for determining free and reduced price meal eligibility may disclose, without parental consent all eligibility information to persons directly connected with the administration or enforcement of a federal or state education program as permitted by section 9(b)(2)(c)(iii) of the Richard B. Russell National School Lunch Act, including:

1. Federal, state, and local program operators responsible for the federal or state education program administration or compliance and their contractors, e.g., National Assessment of Educational Progress ("NAEP"). Note: Only eligibility status may be disclosed without consent to other federal/state/local education programs, e.g., NCLB, Race to the Top.

2. Medicaid Schools Program if the services are included in the IEP for Medicaid-eligible students). Note: Prior notice to parents is required and parents may decline to have their information disclosed.

3. Federal, state or law enforcement agencies investigating violations of school meals programs or any programs authorized to have access to names and eligibility status.

4. Comptroller General of the U.S. for audit and evaluation purposes.

D. Unauthorized disclosure of a student's name or eligibility status is punishable by a fine of not more than $1,000 or imprisonment for up to one year, or both.

> **Caveat/Practice Pointer** - School officials should have procedures in place to limit access to the child's eligibility status to as few individuals as possible, to provide access only to those who have a need to know the information and a method of notifying parents when the school district plans to disclose or use eligibility information, either as a general notification of potential disclosure or a specific notification to disclose information to a particular program. Parents must be given the option to elect not to have their child's information disclosed.

VIII. Children's Internet Protection Act ("CIPA"), 47 U.S.C. 254(h) and (l)).[7]

A. CIPA is a federal law enacted to address concerns about access to offensive content over the Internet on computers of any school (or library) that receives funding for Internet access or internal connections from the E-rate program, a program that makes certain communications technology more affordable for eligible entities.

B. Schools subject to CIPA are required to adopt and implement an Internet safety policy as provided in the final regulations issued September 13, 2011. 76 Fed. Reg. 56295 *et seq.*; 47 C.F.R. § 54.520(c)(1)(I); 47 U.S.C. 254(h).

1. Schools, beginning July 1, 2012, must enact policy to educate minors (defined as children who have not yet attained age 17) about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. The Federal Communications Commission did not define "social networking" or "cyberbullying."

2. Schools must use specific technology to filter or block certain Internet access by both adults and minors to visual depictions that are obscene, child pornography, or, with respect to use of the computers by minors, harmful to minors. and must monitor the online activities of minors.

[7] Another law, the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6508 (1998), 16 C.F.R. Part 312 (effective April 21, 2000) applies to operators of commercial websites and online services directed to children under 13 that collect, use, or disclose personal information from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children. While it does not apply to website operators that contract with schools to provide online services involving the collection, use or disclosure of students' personal information such as homework help lines or web-based testing services because collecting such information is for the use and benefit of the school, and for no other commercial purpose, the law does allow, but does not require, schools to act as agents for parents in providing consent for the online collection of students' personal information within the school context. See Statement of Basis and Purpose, 64 Fed. Reg. 59888, et seq., available at www.ftc.gov/os/1999/10/64fr59888.pdf, p. 59904.

C. CIPA also requires the adoption and implementation of policies concerning unauthorized access (e.g., "hacking") and unauthorized disclosure, use, and dissemination of personal information regarding minors. 47 U.S.C. §254(l)(1)(A).

Caveat/Practice Pointer - It is the school board's discretion as to how it will comply with CIPA. School district policy purposes should be to a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communication; b) to prevent unauthorized access and other unlawful online activity; c) to prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and to comply with CIPA.