National Association of College and University Attorneys

Presents:

FERPA: The Basics and Beyond

Virtual Seminar

In cooperation with the American Council on Education (ACE) and the National Association of Student Personnel Administrators (NASPA)

Wednesday, October 8, 2014

12:00 PM – 2:00 PM Eastern
11:00 AM – 1:00 PM Central
10:00 AM – 12:00 PM Mountain
9:00 AM – 11:00 AM Pacific

Presenters:

Jeffery Graves
University of Texas at Austin

Steven McDonald
Rhode Island School of Design

HAVE A QUESTION?

ASK IT NOW!

If you'd like to submit a subject matter-related question to the presenters prior to the program, please submit your question using our online question box.

If time permits, NACUA staff will make every effort to pose your question to the panelists during the virtual seminar, but please note that they may not be able to address all questions.

You will also have an opportunity to pose questions during the program, but seeing your questions in advance will help the presenters focus on the material that is most relevant to the audience.

NACUA VIRTUAL SEMINAR SERIES

WEDNESDAY, OCTOBER 8, 2014

FERPA: THE BASICS AND BEYOND

ATTENDANCE RECORD

Organization: _____

All participants are asked to sign-in, but if you are an attorney applying for Continuing Legal Education credits (CLEs), you ***must*** sign this attendance sheet to verify your attendance at this seminar. After completion, please return this form to NACUA (clecredit@nacua.org). ***Total CLE Credits = 120 minutes**

	PRINT Your Name	**SIGN Your Name**	**Bar Number** *(If Applying for CLE)*
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			
12.			
13.			
14.			
15.			
16.			
17.			
18.			
19.			
20.			

NACUA VIRTUAL SEMINAR SERIES

WEDNESDAY, OCTOBER 8, 2014

FERPA: THE BASICS AND BEYOND

CERTIFICATE OF ATTENDANCE

- **Attorneys from Connecticut, Maryland, Massachusetts, Michigan, South Dakota or the District of Columbia:** These jurisdictions do not have CLE requirements and therefore require no report of attendance or filing.
- **Attorneys from California, Illinois, New Jersey, New York or Tennessee:** Do not return this form to NACUA. Please keep this form for your records to submit directly to your state CLE commission or in case your state bar audits you for CLE compliance. Please also remember to sign the site roster, indicating your attendance, before you leave.
- **Attorneys from all other states:** Please complete and return this form no later than TODAY to NACUA (clecredit@nacua.org). Please also remember to sign the site roster, indicating your attendance, before you leave.

NACUA certifies that this program has been presumptively approved and conforms to the standards prescribed by the rules and regulations of the State Bars of AZ, AR, CA, CO, DE, HI, MO, NV, NH, NJ, NM, NY, RI, VT, WV and WY. NACUA will apply for CLE credits from the following states: AL, AK, FL, GA, ID, IL, IN, IA, KS, KY, LA, ME, MN, MS, MT, NC, ND, OK, OR, SC, TN, TX, UT, VA, WA and WI) Note: Restrictions vary state by state and not all states will accredit this virtual seminar.

Upon receipt of this certificate of attendance and your site roster, NACUA will process the credits through the applicable state if approved.

CERTIFICATION

By signing below, I certify that I attended the above activity and request 120 minutes of CLE credits.

Name _____ Bar Number _____

Address _____ Email _____

Signature _____ Date _____

Authorized By:

Meredith L. McMillan

Meredith McMillan, CMP
NACUA Meetings and Events Planner

WEDNESDAY, OCTOBER 8, 2014

FERPA: THE BASICS AND BEYOND

SPEAKER BIOGRAPHIES

Jeffery L. Graves is a 1991 graduate of the University of Texas at Austin's School of Law and currently is an Associate Vice President for Legal Affairs at the University of Texas at Austin. Mr. Graves is also the university's Privacy Officer. Mr. Graves has practiced higher education law for over twenty years and has been a member of NACUA since 1995. Prior to joining UT's Office of Legal Affairs in 2001, Mr. Graves was a shareholder with the Albuquerque, New Mexico law firm Sutin, Thayer and Browne, P.C. where he practiced employment law and higher education law.

Steven J. McDonald is General Counsel at Rhode Island School of Design and previously served as Associate Legal Counsel at The Ohio State University. He is the editor of The Family Educational Rights and Privacy Act: A Legal Compendium; the author of articles on FERPA for the Chronicle of Higher Education, Inside Higher Education, and other publications; and a frequent speaker on FERPA. He also is a Fellow and past member of the Board of Directors of NACUA. In State, ex rel. Thomas v. The Ohio State University, the Ohio Supreme Court ruled that he really is a lawyer. He received his A.B. from Duke University and his J.D. from The Yale Law School.

NACUA

FERPA: The Basics and Beyond

Presented by the National Association of College and University Attorneys

In cooperation with the American Council on Education (ACE) and the National Association of Student Personnel Administrators (NASPA)

Jeffery Graves
University of Texas at Austin

Steven McDonald
Rhode Island School of Design

NACUA OCTOBER 8, 2014 VIRTUAL SEMINAR

NACUA

FERPA Basics: An Overview of the Structure of FERPA

Steve McDonald
Rhode Island School of Design

2

NACUA

FERPA

- The Family Educational Rights and Privacy Act of 1974
- A.K.A. the Buckley Amendment

3

NACUA

FERPA's Big Three

- College students have the right, in general, to:
  - Control the disclosure of their "education records" to others
  - Inspect and review their own "education records"
  - Seek amendment of their "education records"

4

NACUA

FERPA Basics: Key Definitions

Jeff Graves
University of Texas at Austin

Steve McDonald
Rhode Island School of Design

5

NACUA

So, What's an "Education Record"?

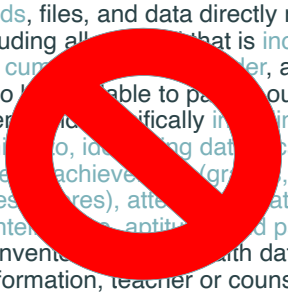
- "[O]fficial records, files, and data directly related to [students], including all material that is incorporated into each student's cumulative record folder, and intended for school use or to be available to parties outside the school or school system, and specifically including, but not necessarily limited to, identifying data, academic work completed, level of achievement (grades, standardized achievement test scores), attendance data, scores on standardized intelligence, aptitude, and psychological tests, interest inventory results, health data, family background information, teacher or counselor ratings and observations, and verified reports of serious or recurrent behavior patterns."

6

NACUA

So, What's an "Education Record"?

- "[O]fficial records, files, and data directly related to [students], including all ... that is incorporated into each student's cum... ...der, and intended for school use or to ... able to pa... outside the school or school syster... ...ifically in... ...ing, but not necessarily limi... ...o, id... ...ng dat... ...cademic work completed, leve... achieve... (gr... , standardized achievement tes... ...res), atte... ...ata, scores on standardized inte... ... aptitu... ...d psychological tests, interest invent... ...ith data, family background information, teacher or counselor ratings and observations, and verified reports of serious or recurrent behavior patterns."



7

NACUA

So, What's an "Education Record"?

- "'Education records' . . . means those records that are:
  (1) Directly related to a student; and
  (2) Maintained by an educational agency or institution or by a party acting for the agency or institution"

8

NACUA

So, What's an "Education Record"?

- "'Education records' . . . means those records that are:
  (1) Directly related to a student; and
  (2) Maintained by an educational agency or institution or by a party acting for the agency or institution"

9

NACUA

So, What's an "Education Record"?

- "'Record' means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche"
- N.B.: Does not include information that is not "recorded" – that is, personal knowledge

10

NACUA

So, What's an "Education Record"?

- In general, a record is "directly related" to a student if it contains "personally identifiable information" about that student
  - *Possible* exception if student is truly tangential to the record

11

NACUA

So, What's an "Education Record"?

- "'Personally identifiable information' includes, but is not limited to"
  - The name of the student or of the student's parent or other family member
  - The address of the student or student's family
  - Personal identifiers such as SSNs, student numbers, or biometric records
  - Other indirect identifiers such as date or place of birth or mother's maiden name

12

NACUA

So, What's an "Education Record"?

– "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"

13

NACUA

So, What's an "Education Record"?

– "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"

14

NACUA

So, What's an "Education Record"?

- "Maintain" is *not defined*!
- *Owasso Independent School District v. Falvo*, 534 U.S. 426 (2002):
  - "FERPA implies that education records are institutional records kept by a single central custodian, such as a registrar."
  - "The ordinary meaning of the word 'maintain' is 'to keep in existence or continuance; preserve; retain.'"
- Requires conscious decision on the part of the institution?

15

NACUA

We Don't Need No "Education"

- "Education records" certainly includes transcripts, exams, papers, and the like
- But it also includes:
  - Financial aid and account records
  - Disability accommodation records
  - Disciplinary records
  - Photographs
  - Faculty and staff e-mail messages to, from, or about a student
  - *Virtually everything!*

16

NACUA

What are *not* "education records?"

- Sole possession records
- Law enforcement records
- Certain employment records
- Treatment records
- Alumni records
- Peer graded papers

17

NACUA

What are *not* "education records?"

Sole Possession Records

- Records that are kept in the sole possession of the maker;
- Used only as a personal memory aid; and
- Not accessible or revealed to any other person except a temporary substitute for the maker of the record.

Example: A teacher's personal annotated seating chart.

18

NACUA

What are *not* "education records?"

Records of the law enforcement unit of the institution:

- The law enforcement unit must be commissioned police or non-commissioned guards who enforce the law or maintain security;
- The law enforcement unit may also perform non-law enforcement functions such as investigations of student misconduct;

19

NACUA

What are *not* "education records?"

Records of the law enforcement unit of the institution (continued):

- Records must be created by the law enforcement unit at least in part for a law enforcement purpose; and
- Must be maintained by the law enforcement unit.
- Does ***not*** include copies of law enforcement records maintained by another part of the institution; or
- Records of a law enforcement unit created for a non-law enforcement purpose.

20

NACUA

What are *not* "education records?"

Employment Records

- Records related solely to an employee who also happens to be a student, so long as the employee is not employed because of their status as a student.
- Conversely, the employment records of employees who are employed as a result of their student status, e.g., work study, teaching assistants, graduate assistants, etc., ***are*** education records and subject to FERPA.

21

NACUA

What are *not* "education records?"

Treatment Records

- Records "made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity";
- Made, maintained, or used only in connection with treatment of the student and disclosed only to those providing treatment.

22

NACUA

What are *not* "education records?"

Treatment Records (continued)

- The Health Insurance Portability and Accountability Act (HIPAA) excepts from its coverage education records subject to FERPA as well as treatment records subject to this exception.
- The student's access to such treatment records is therefore subject to your state's law regarding medical records.

23

NACUA

What are *not* "education records?"

Alumni Records

- "Records created or received by an educational agency or institution after an individual is no longer a student in attendance and
- that are not directly related to the individual's attendance as a student."
- Records that are created after a student is no longer in attendance but relate to the student's attendance ***are*** subject to FERPA, e.g., a post-graduation academic misconduct proceeding.

24

NACUA

What are *not* "education records?"

Peer graded papers

- *Owasso Independent School District v. Falvo*, 534 U.S. 426 (2002)
- The Supreme Court decided that peer graded assignments were not "maintained" by the institution at that point and that the students doing the grading were not "acting for" the institution.

25

NACUA

FERPA Basics: Permitted Disclosures

Jeff Graves
University of Texas at Austin

Steve McDonald
Rhode Island School of Design

26

NACUA

Disclosure

- Before disclosing education records – or information from education records – an institution must obtain a signed and dated written consent from *all* relevant students, specifying:
  - The records that may be disclosed
  - The purpose for which they may be disclosed
  - The persons or classes to whom they may be disclosed

27

NACUA

Disclosure Without Student Consent

The relevant regulation, 34 CFR 99.31, lists sixteen instances in which FERPA-protected student information may be disclosed without consent. We will address in detail some of the more common ones today.

- Directory information
- School officials with a legitimate educational interest
- Parents
- Threat to health or safety
- Litigation
- Audits and evaluation

28

NACUA

Disclosure Without Student Consent

"Directory Information" is information that would not generally be considered harmful or a violation of privacy if disclosed. Within certain parameters, it is defined by the institution and so can vary among institutions. For example, photos may be defined as directory information, but an institution is not required to define photos as such.

- The institution must provide the definition of directory information in its annual notice to students.
- Students must be allowed to "opt out" of disclosure of directory information.

29

NACUA

Disclosure Without Student Consent

"Directory Information" may include but is not limited to:

- name, address, telephone listing, email address, photograph, date and place of birth, major, grade level, enrollment status, dates of attendance, participation in sports and weight and height of team members, degrees, honors and awards received, most recent institution attended, and other similar information.
- As you would expect, certain things, like social security numbers, may never be included in the definition.

30

NACUA

Disclosure Without Student Consent

School Officials

- Disclosure of personally identifiable information ("PII") may be made to "other school officials, including teachers" when they have a "legitimate educational interest".
- A school official has a "legitimate educational interest" if they need the information to fulfill their professional responsibilities for the institution.
  - this includes both academic duties and non-academic business duties
- Again, notice must be given to students in the institution's policy and annual FERPA notice that such disclosures will be made.

31

NACUA

Disclosure Without Student Consent

School officials (continued)

Vendors, contractors and other outside entities may be considered school officials with a legitimate educational interest.

- Must be performing a function the institution would otherwise have to perform itself
- Must be under the control of the institution with regard to use of the information
- Cannot redisclose the information to anyone without the student's permission
- May use the information only for the purpose for which it was disclosed

32

NACUA

Disclosure Without Student Consent

Parents

Parents *may* have their student's PII disclosed to them:

- If the student is their dependent for federal income tax purposes;
- If the student is under 21 at the time of disclosure and the institution has found that the student violated either a law or institutional policy governing the use of possession of alcohol or controlled substances in a disciplinary proceeding; or
- In a health or safety emergency

33

NACUA

Disclosure Without Student Consent

Threat to Health or Safety

- PII may be disclosed to "appropriate parties, including parents...in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals."
- Must be an articulable and significant threat.
- May disclose only to those whose knowledge of the information is necessary to protect the health or safety of the student or others.
- Must have a "rational basis" for the disclosure based on the information available at the time of the disclosure.

34

NACUA

Disclosure Without Student Consent

Litigation

- A student's PII may be disclosed to a court without a subpoena or court order when a student has initiated "legal action" and the disclosure is relevant to the institution's defense.
- An institution who is a non-party to litigation may provide PII pursuant to a judicial order or lawfully issued subpoena after making a reasonable effort to notify the student in advance of production so that the student may seek protective action.
  - unless the subpoena or order is for a law enforcement purpose and its existence has been ordered not to be disclosed.

35

NACUA

Disclosure Without Student Consent

Audits and Evaluations of Federal or State Supported Programs

- Student PII may be disclosed to State Educational Authorities (SEAs) or Local Educational Authorities (LEAs) or their "authorized representatives" to perform audits or evaluations of federal or state supported programs.
- An authorized representative is any individual or entity designated by the SEA or LEA and with whom there is a written agreement that specifies what PII will be disclosed and how it will be used, a description of the authorized representative's activities sufficient to make clear it is an audit or evaluation, procedures to protect the PII, and a record destruction requirement and schedule.

36

NACUA

Disclosure Without Student Consent

Other Permissible Non-consensual Disclosures of PII

- To another institution "where the student seeks or intends to enroll";
- To the student him or herself;
- Disclosure of final results of a disciplinary hearing in which a student was found to have committed acts that would constitute a crime of violence or non-forcible sex offense;
- Disclosure to the alleged victim of the final results of a disciplinary hearing in which a student was alleged to have committed acts that would constitute a crime of violence or non-forcible sex offense;
- Disclosures in connection with the student's financial aid;

37

NACUA

Disclosure Without Student Consent

Other Permissible Non-consensual Disclosures of PII (continued)

- To accrediting organizations;
- To organizations conducting studies for or on behalf of institutions to develop, validate or administer predictive tests, administer student aid programs or improve instruction;
- The disclosure concerns registered sex offenders and consists of information provided to the institution pursuant to law.

38

NACUA

Practical Tips

- Posting grades
  - Only by anonymous number in non-alphabetical order
  - Better yet, by authenticated web portal
- Returning exams and papers
  - No self-serve pick-up
- Talking to parents
  - Check student status first
  - Confirm they really are the parents
  - And remember that you don't have to at all . . . .

39

NACUA

Practical Tips

- Be careful what you write down about your students
  - Or at least be careful about sharing it
  - "Three may keep a secret, if two of them are dead."
- Be careful how you dispose of it
- Be particularly careful with e-mail, other electronic communications, and digital storage

40

NACUA

FERPA Basics: Inspection and Review

Steve McDonald
Rhode Island School of Design

41

NACUA

Inspect and Review

- Must allow students to "inspect and review" their own education records within 45 days of request
- Need not provide copies unless "circumstances effectively prevent the . . . student from exercising the right to inspect and review"
- The *only* exceptions are financial aid records of parents and confidential letters of recommendation to which the student has waived access
- If record relates to more than one student, must redact portions relating to other students

42

NACUA

FERPA Basics: Amendment

Jeff Graves
University of Texas at Austin

NACUA

Requesting Amendment

If a student believes the information in her records is inaccurate, misleading, or in violation of the student's rights of privacy, she may request amendment.

- The institution must decide to amend or not within a "reasonable time."
- If the institution decides not to amend, it must inform the student of the decision and the right to a hearing to appeal the decision not to amend.

NACUA

Amendment Hearing Results

- If after a hearing the institution decides that the information was inaccurate, misleading, or in violation of the student's rights of privacy, it shall amend the record and notify the student.
- If the institution decides the record was accurate, it shall notify the student and give the student the right to place a statement in the record stating why she disagrees with the information in the record.
- Such statement must remain with the record and be disclosed whenever the contested part of the record is disclosed.

45

NACUA

Conduct of the Amendment Hearing

The amendment hearing must meet the following minimum requirements:

- The hearing must be held within a "reasonable time" after the request for a hearing;
- The institution must provide the student with notice of the date, time, and place, reasonably in advance of the hearing;
- The hearing must be conducted by an individual who does not have a direct interest in the outcome;
- The hearing must give the student a full and fair opportunity to present evidence relevant to the issues raised by the student;
- The hearing must be decided solely on the evidence presented, and must include a summary of the evidence and the reasons in the decision.

46

NACUA

FERPA Basics: Enforcement

Steve McDonald
Rhode Island School of Design

NACUA

Enforcement

- No private right of action
- FPCO may terminate an institution's education-related federal funding, or take "any [other] legally available enforcement action," if, *but only if*:
  - The institution violates FERPA, *and*
  - The violation represents a "policy or practice," *and*
  - "[C]ompliance cannot be secured by voluntary means" within a reasonable period of time

48

NACUA

Questions and Answers

NACUA

Applied FERPA: Teaching and Working in the Cloud

Steve McDonald
Rhode Island School of Design

50

NACUA

U-Tube?

- May schools:
  - Outsource e-mail?
  - Use cloud-based service providers to process or store education records?
- May faculty require:
  - Participation on listservs?
  - Blog posts?
  - Use of online portfolios?
  - Creation and posting of videos?
  - Use of other social media?

51

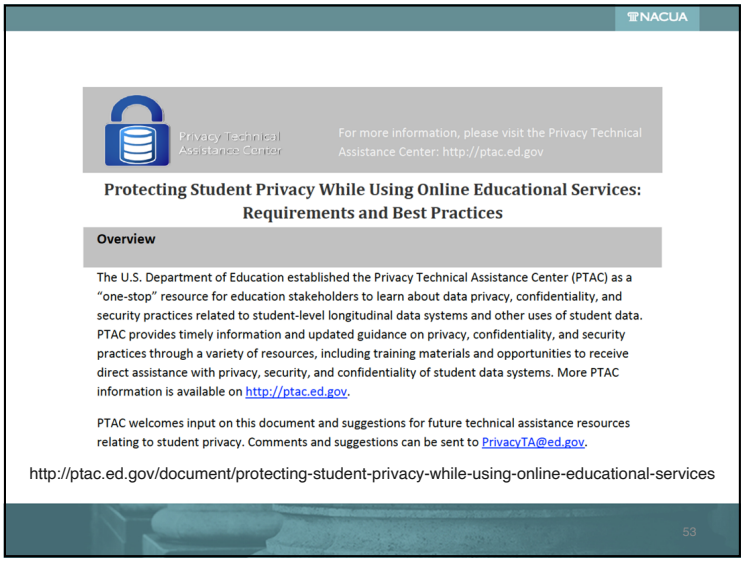
NACUA

First Things First

- FERPA applies to educational institutions and their agents, not to students and not to external social media and other services
  - Including (most) MOOCs
  - At least as far as FERPA is concerned, students are free to post whatever they want wherever they want whenever they want
- Schools/faculty may post directory information anywhere they want (for non-opt-outs)
- Schools/faculty may outsource services and provide education records to cloud providers that agree to act as "school officials"

52

NACUA



http://ptac.ed.gov/document/protecting-student-privacy-while-using-online-educational-services

53

NACUA

FPCO Guidance

- "[T]he framework under which the school or district uses the service must satisfy the 'direct control' requirement by restricting the provider from using the PII for unauthorized purposes. . . . If the school or district has shared information under FERPA's school official exception, . . . the provider cannot use the FERPA-protected information for any other purpose than the purpose for which it was disclosed. . . . [T]he provider may not share (or sell) FERPA-protected information, or re-use it for any other purpose, except as directed by the school or district and as permitted by FERPA."

54

NACUA

FPCO Guidance

- "A provider that has been granted access to PII from education records under the school official exception may use any metadata that are not linked to FERPA-protected information for other purposes, unless otherwise prohibited by the terms of their agreement with the school or district."
  - Is there anything that isn't really linked?

55

NACUA

Hmm?

- Faculty *probably* may require students to use *independent*, external social media and other services
  - Including (most) MOOCs
- But may they require students to use internal social media, and/or may they post student work themselves to either internal or external social media?

56

NACUA

Steve McDonald's "Implied Pedagogical Exception" Theory™

- FPCO: "Neither the statute, the legislative history, nor the FERPA regulations require institutions to depart from established practices regarding the placement or disclosure of student theses so long as students have been advised in advance that a particular undergraduate or graduate thesis will be made publicly available as part of the curriculum requirements."

57

NACUA

Steve McDonald's "Implied Pedagogical Exception" Theory™

- FPCO: "The final regulations . . . ensure that . . . students [may] not use the right to opt out of directory information disclosures to remain anonymous in the classroom, by clarifying that opting out does not prevent disclosure of the student's name, institutional e-mail address, or electronic identifier in the student's physical or electronic classroom."

58

NACUA

Steve McDonald's "Implied Pedagogical Exception" Theory™

- *Owasso*: "We doubt Congress meant to intervene in this drastic fashion with traditional state functions. Under the Court of Appeals' interpretation of FERPA, the federal power would exercise minute control over specific teaching methods and instructional dynamics in classrooms throughout the country. The Congress is not likely to have mandated this result, and we do not interpret the statute to require it."

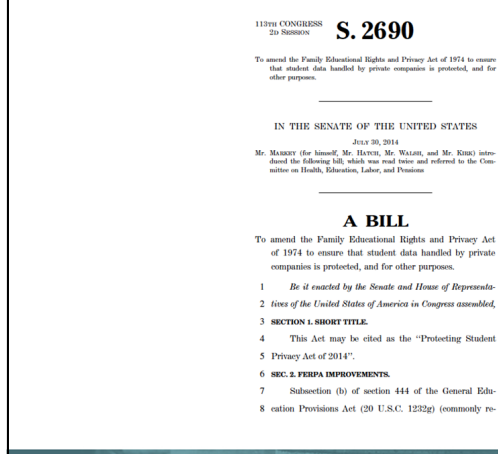
59

NACUA

Can v. May v. Should

- What is the pedagogical reason for requiring the posting to be public?
- If there is one, is it really important that the posting be attributed?
- What are the implications for the student's privacy?
- What are the implications for the student's intellectual property?
- Who's reading the contracts and terms of service?

60



113TH CONGRESS
2D SESSION

S. 2690

To amend the Family Educational Rights and Privacy Act of 1974 to ensure that student data handled by private companies is protected, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JULY 30, 2014

Mr. MARKEY (for himself, Mr. HATCH, Mr. WALSH, and Mr. KIRK) introduced the following bill; which was read twice and referred to the Committee on Health, Education, Labor, and Pensions

A BILL

To amend the Family Educational Rights and Privacy Act of 1974 to ensure that student data handled by private companies is protected, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Protecting Student Privacy Act of 2014".

SEC. 2. FERPA IMPROVEMENTS.

Subsection (b) of section 444 of the General Education Provisions Act (20 U.S.C. 1232g) (commonly re-

Applied FERPA: Campus Safety and Discipline

Jeff Graves
University of Texas at Austin

NACUA

FERPA and the Clery Act

Crime reporting obligations under Clery

- Campus law enforcement officers, non-law enforcement campus security officers (security guards) and local law enforcement officers will normally collect full details of crimes, including PII.
- However, in reporting to the institution for Clery reporting purposes, campus security officers do not have to report PII, although they may do so in order for the institution to pursue disciplinary charges against alleged perpetrators separate from the criminal process.
- Campus security officers need to use PII in issuing a timely warning.

63

NACUA

FERPA and the Clery Act

Crime reporting obligations under Clery (continued)

- Other mandatory reporting CSAs, such as resident assistants and student judicial services personnel, are not required by the Clery Act to disclose PII. Once student PII related to a Clery report is disclosed to institutional officials, it becomes FERPA protected.
- The Clery mandated annual security report does *not* require PII be disclosed. Rather, it requires institutions to provide statistics for certain specified crimes that occurred on campus or on contiguous property.

64

NACUA

FERPA and the Clery Act

Results of Disciplinary Proceedings

- Clery mandates that institutions have procedures in place for simultaneously notifying the accuser and accused of the outcome of disciplinary proceedings.
- FERPA expressly allows disclosure to the alleged victim of the final results of a disciplinary hearing in which a student was alleged to have committed acts that would constitute a crime of violence or non-forcible sex offense without consent.

65

NACUA

FERPA and the Clery Act

Results of Disciplinary Proceedings (continued)

- Final results are the name of the accused, the findings, the sanction, and the rationale for the findings and sanction.
  - Any other student names may only be included with the consent of that student

66

NACUA

FERPA and the Clery Act

Timely Warnings and FERPA

- The Clery Act mandates that institutions must provide the campus community with a timely warning about a reported crime that the institution believes represents a continued threat to students and employees.
  - e.g., a sexual assault where the assailant is unknown and not apprehended
- In some instances, for example when an identified student is an alleged perpetrator of a crime of violence and remains at large, a timely warning may need to include PII. In these instances, FERPA's health and safety exception will allow the disclosure.

67

NACUA

FERPA and Title IX

In Case of Conflict, Title IX Trumps FERPA

- The General Education Provisions Act (GEPA), of which FERPA is a part, states that nothing in GEPA "shall be construed to affect the applicability of ...Title IX of Education Amendments of 1972..." *20 U.S.C. § 1221(d*).
- The Department of Education interprets this provision to mean that FERPA continues to apply in the context of Title IX enforcement, but if there is a direct conflict between the requirements of FERPA and the requirements of Title IX, the requirements of Title IX override any conflicting FERPA provisions.

68

NACUA

FERPA and Title IX

Notice of Outcome

- When sexual violence is found to have occurred, Title IX requires - among other things - a school to tell the complainant any sanctions imposed on the perpetrator that directly relate to the complainant.
- This includes, but is not limited to:
  - requiring that the perpetrator stay away from the complainant until both parties graduate
  - prohibiting the perpetrator from attending school for a period of time
  - transferring the perpetrator to another residence hall, other classes, or another school

69

NACUA

FERPA and Title IX

Notice of Outcome (continued)

- This falls within FERPA's exception for disclosure to the alleged victim of the final results of a disciplinary hearing in which a student was alleged to have committed acts that would constitute a crime of violence or non-forcible sex offense without consent.

70

NACUA

FERPA, Title IX, and Disciplinary Proceedings

Disclosures during a Title IX disciplinary proceeding must be consistent with FERPA

- If a complainant requests confidentiality or that an investigation not move forward, an alleged perpetrator will still have a right to inspect those portions of the complaint that directly relate to him or her.
  - Identifying information of other students must be redacted.

71

NACUA

FERPA, Title IX, and Disciplinary Proceedings

Disclosures during a Title IX disciplinary proceeding must be consistent with FERPA (continued)

- Pursuant to Title IX, both the complainant and respondent must have similar access to information that will be used at a hearing, so long as it is relevant to proving or defending against the allegation and so long as access is provided as consistent with FERPA as possible.
  - e.g., "character evidence" derived from information contained in education records should not be shared with the other party

72

NACUA

FERPA and Other Disciplinary Proceedings Issues

Public Universities and Constitutional Due Process

- When a student at a public university faces a disciplinary proceeding that implicates a property interest, such as when expulsion is a possible sanction, the student's right to due process may conflict with the institution's FERPA obligations.
- In such a case of direct conflict, the due process constitutional principle controls.
  - e.g., a respondent likely has a right to know the identity of all possible witnesses, not just those that will be called at the hearing

73

NACUA

Applied FERPA: Public Records

Jeff Graves
University of Texas at Austin

NACUA

FERPA and Open Records Laws

- FERPA is not a mandatory disclosure law
- Most exceptions to FERPA's general mandate that disclosures require consent are permissive.
  - e.g., an institution *may* disclose information without consent to a parent of a student who is a dependent for federal tax purposes, but is not required to do so
- However, broad state open records laws may render disclosure of records mandatory once the records are no longer confidential under FERPA.
- Contrary view: FERPA trumps the state open records law and gives the institution the discretion to disclose or not when an exception applies.

75

NACUA

Questions and Answers

NACUA

Thank you!

The NACUA FERPA resource page is located at:
http://www.nacua.org/lrs/NACUA_Resources_Page/FERPAResources.asp

The Higher Education Compliance Alliance Privacy/Student Records resource page is located at:
http://www.higheredcompliance.org/resources/privacy-student-records.html

THE FUNDAMENTALS OF FUNDAMENTAL FERPA

June 22, 2014

Steven J. McDonald
General Counsel
Rhode Island School of Design

I. BACKGROUND AND BASICS

Enacted as a seemingly inconsequential floor amendment having little to do with higher education, the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g, popularly known as "FERPA" or the "Buckley Amendment," nevertheless quickly became one of the mainstays of college and university law practice. And although it still tends to inhabit only the remotest fringes of our consciousness most of the time, it is fair to say that FERPA is relevant to virtually everything we do on our campuses. Thus, it is appropriate to "refresh" our understanding of its requirements every once in a while, and there is no time like the present.

Congress enacted FERPA in response to a growing public awareness of and concern about the public dissemination by primary and secondary schools of information commonly considered private in nature, the withholding of "secret files" on students, and recordkeeping practices in general. Much like other "records" statutes of that era, it reflected a desire to give a measure of control to the subjects of government records – in this case, "education records." In very general terms, then, FERPA gives college students the rights to:

1. Control the disclosure of their "education records" to others;
2. Inspect and review their own "education records;" and
3. Seek amendment of their "education records."

Unlike at the primary and secondary level, these rights belong to the student, and not to the student's parents or legal guardians, regardless of the student's age. Moreover, the rights continue to exist after the student's graduation and expire only upon either the destruction of the relevant records or the student's death.

II. KEY DEFINITIONS

All of FERPA revolves around the central term "education records,"[1] which is defined in the implementing regulations as follows:

"Education records" . . . means those records that are:

(1) Directly related to a student; and

[1] The commonly used variant "educational records" is both incorrect – it does not exist in the statute or regulations – and misleading. While records that are "educational" in nature, such as student papers, exams, and transcripts, certainly are covered by FERPA, so are a multitude of records that have nothing whatever to do with "academics." Banish the term from your vocabulary.

(2) Maintained by an educational agency or institution or by a party acting for the agency or institution.

34 C.F.R. § 99.3 (emphasis added).

To fully understand that definition requires an understanding of the further definitions of each of the underlined terms, and a few more:

"Educational institution": "any public or private . . . institution" that receives funds "under any program administered by the Secretary [of Education]," most notably including the various federal financial aid programs. 34 C.F.R. §§ 99.1 and 99.3. In other words, pretty much every institution of higher education.

"Record": "any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche." 34 C.F.R. § 99.3. Thus, the manner or form in which information is recorded is irrelevant; not only paper records, but also electronic records, photographs, videotapes, and even hand-carved stone tablets are covered. Note, however, that information that is not recorded anywhere other than in your brain – that is, personal knowledge – is not a "record," and thus not an "education record," and thus not subject to FERPA. (Be careful when dealing with information that is both within your personal knowledge and recorded in some other format, however, as it will not always be clear which you are relying on.)

"Student": "any individual who is or has been in attendance at an educational . . . institution." 34 C.F.R. § 99.3. The term does not include applicants, who thus are not protected by FERPA unless and until they are admitted and "attend," thereby becoming "students." If they do, FERPA not only applies to their records going forward, but also "reaches back" and brings their application records within its scope.

"Attendance": "includes, but is not limited to . . . [a]ttendance in person or by paper correspondence, videoconference, satellite, Internet, or other electronic information and telecommunications technologies for students who are not physically present in the classroom." 34 C.F.R. § 99.3. Each institution has discretion to define when, between admission and the first day of classes, a student is first considered to be "in attendance."

"Directly related": The term is not defined in either the statute or the regulations, but, under long-standing interpretation of the Family Policy Compliance Office, the office within the Department of Education charged with overseeing FERPA, a record generally is considered to be "directly related" to a student if it contains "personally identifiable information" about that student.

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

(a) The student's name;

(b) The name of the student's parent or other family members;

(c) The address of the student or student's family;

(d) A personal identifier, such as the student's social security number, student number, or biometric record;

(e) Other indirect identifiers, such as the student's date of birth, place of birth, or mother's maiden name;

(f) 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; or

(g) Information requested by a person who the educational . . . institution reasonably believes knows the identity of the student to whom the education record relates."

34 C.F.R. § 99.3.

"Maintained": Although this term may be the most critical of all – especially when it comes to determining the status of, say, student e-mail messages that are stored in the student's account on an institutional server – it is not defined in either the statute or the regulations. In *Owasso Independent School District v. Falvo*, 534 U.S. 426, 435 (2002), the Supreme Court noted – tantalizingly – that "FERPA implies that education records are institutional records kept by a single central custodian, such as a registrar," but ultimately declined to define "maintain" that narrowly, or, really, to give much of any guidance on the question at all. Thus, for now, it is unclear whether a record is "maintained" by an educational institution whenever it is in the possession, custody, or control of any employee or agent of the institution, or, rather, only when an employee or agent of the institution has made a conscious decision to "maintain" the record for the institution's own purposes. I personally believe that the answer is, and should be, the latter, but there is no clear authority to that effect.

In short, given the vast breadth of its various components, the term "education records" includes not only such standard "academic" records as student transcripts, papers, and exams, but also virtually <u>any</u> information about a student in <u>any</u> record that is "maintained" by the institution. The only such records that are specifically excluded from the scope of the term, and that therefore are not subject to the (full panoply of) restrictions of FERPA, are the following:

"Sole possession" records: "Records that are kept in the sole possession of the maker, are used only as a personal memory aid, and are not accessible or revealed to any other person except a temporary substitute for the maker of the record." 34 C.F.R. § 99.3. For example, the private notes a professor may keep about class participation over the course of a semester, for consultation when it comes time to set final grades.

"Law enforcement" records: those records that are "(i) created by [the institution's] law enforcement unit [including non-commissioned public safety or security offices]; (ii) created [at least in part] for a law enforcement purpose; and (iii) maintained by the law enforcement unit." 34 C.F.R. §§ 99.3 and 99.8 (emphasis added). Records that are generated by others and sent to the law enforcement unit – say disciplinary records from the institution's judicial affairs office – are not "law enforcement" records and remain covered by FERPA even when in the law enforcement unit's hands. If the law enforcement unit discloses law enforcement records to others – which it is free to do, because they are not subject to FERPA – metaphysical things begin to happen: The law enforcement unit's copies of those records remain free from FERPA restrictions, as do any copies that it discloses to the general public, but any copies that end up in the hands of other institutional employees or agents become transformed into "education records" subject to the full panoply of FERPA restrictions.

"Employment" records: records related solely to the employment of a "student" by the institution, provided that the student is not "employed as a result of his or her status as a student." 34 C.F.R. § 99.3. In other words, if being a student is part of the job description and requirements – a work-study or GTA/GRA position, for example – any employment records concerning the student who holds the position are "education records" and thus subject to FERPA. This exclusion was intended primarily to keep the employment records of institutional employees who happen to take classes from becoming "education records." Records pertaining to such employees' *student* status *are* "education records," however.

"Treatment" records: records that are "(i) made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his or her professional capacity or assisting in a paraprofessional capacity; (ii) made, maintained, or used only in connection with treatment of the student; and (iii) disclosed only to individuals providing the treatment." 34 C.F.R. § 99.3. Although such records are not subject to FERPA, the final part of this definition nevertheless effectively prohibits an institution from disclosing them other than in accordance with FERPA – a seeming paradox that is the entire basis for the general exclusion of student medical records from the privacy provisions of HIPAA. (In effect, such records really are exempt only from the "inspect and review" part of FERPA. That issue is deferred to state law on patients' right of access to their medical records.)

"Alumni" records: "Records created or received by an educational . . . institution after an individual is no longer a student in attendance and that are not directly related to the individual's attendance as a student." 34 C.F.R. § 99.3. This exception is intended primarily to cover the sorts of records generated by an institution's alumni office post-graduation. Note, however, that the time a record is created is not determinative; if the information recorded "relates back" to the student's time at the institution, it is still an "education record" even though it was generated after its subject was no longer a "student."

"Peer grades": "Grades on peer-graded papers before they are collected and recorded by a teacher." 34 C.F.R. § 99.3.

III. DISCLOSURE

A. WITH CONSENT

In general, an institution may not disclose "education records" – or information from "education records" – to anyone other than the relevant student unless it first has obtained a signed and dated written consent from the relevant student (or *all* relevant students, if the records are "directly related" to more than one), specifying the records that may be disclosed, the purpose for which they may be disclosed, and the persons or classes of persons to whom they may be disclosed. 34 C.F.R. § 99.30(a) and (b). The requisite consent and signature may be obtained electronically if the method used "identifies and authenticates a particular person as the source of the electronic consent" and "indicates such person's approval of the information contained in the electronic consent." 34 C.F.R. § 99.30(d). An institution that receives a valid consent is not required to disclose the relevant records; the consent gives the institution the discretion to do so, but does not require the institution to do so.

B. WITHOUT CONSENT

In general, an institution may disclose "education records" without such consent only if it first redacts all "personally identifiable information" from the records, 34 C.F.R. § 99.31(b), *or* one of the 16 exceptions enumerated in the regulations applies. Those exceptions are as follows:

1. The disclosure is of "**directory information**," meaning "information . . . that would not generally be considered harmful or an invasion of privacy if disclosed," including, but not limited to, "the student's name; address; telephone listing; electronic mail address; photograph; date and place of birth; major field of study; grade level; enrollment status (e.g., undergraduate or graduate, full-time or part-time); dates of attendance; participation in officially recognized activities and sports; weight and height of members of athletic teams; degrees, honors and awards received; and the most recent educational agency or institution attended." 34 C.F.R. §§ 99.31(a)(11) and 99.3. Social Security Numbers may not be treated as "directory information," but other student ID numbers and user IDs may be treated as "directory information" as long as they cannot be used to gain access to education records without further authentication. 34 C.F.R. § 99.3. To take advantage of this exception, an institution must first give its students notice of the information it has designated as "directory information" – which need not be the full list authorized by the regulations – and an opportunity to "opt out." 34 C.F.R. § 99.37.

   An institution need not provide annual notice of its definitions to alumni, but it "must continue to honor any valid request to opt out

of the disclosure of directory information made while a student was in attendance unless the student rescinds the opt out request." 34 C.F.R. § 99.37(b).

A student may not use the opt-out right "to prevent an . . . institution from disclosing or requiring [the] student to disclose the student's name, identifier, or institutional e-mail address in a class in which the student is enrolled" or from requiring the student "to wear, to display publicly, or to disclose a student ID card or badge that exhibits information" that the institution has properly designated as directory information. 34 C.F.R. § 99.37(c).

An institution may not disclose or confirm directory information about a student if it uses non-directory information (including SSNs) to identify either the student or the records from which the directory information is determined. 34 C.F.R. § 99.37(d).

2. The disclosure is to "**school officials** . . . whom the . . . institution has determined to have **legitimate educational interests**." 34 C.F.R. § 99.31(a)(1). To take advantage of this exception, the institution must give annual notice of its criteria for determining who is a "school official" and what is a "legitimate educational interest." 34 C.F.R. § 99.7(a)(3)(iii). Both definitions can be quite broad. In its model notice, the Family Policy Compliance Office suggests the following language:

> A school official is a person employed by the [School] in an administrative, supervisory, academic, research, or support staff position (including law enforcement unit personnel and health staff); a person serving on the board of trustees; or a student serving on an official committee, such as a disciplinary or grievance committee. A school official also may include a volunteer or contractor outside of the [School] who performs an institutional service of function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of PII from education records, such as an attorney, auditor, or collection agent or a student volunteering to assist another school official in performing his or her tasks.
>
> A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibilities for the [School].

Note that it is the institution, and not the individuals who may wish access, who make these determinations; an institution is free to

deny access to a "school official" who does have a "legitimate educational interest," if the institution determines that there are countervailing policy reasons to do so. Note also that the institution "must use reasonable methods [physical, technological, and/or administrative] to ensure that school officials obtain access to only those education records in which they have legitimate educational interests." 34 C.F.R. § 99.31(a)(1)(ii).

As noted in the model annual notice, "school officials" may include a "contractor, consultant, volunteer, or other party to whom an . . . institution has outsourced institutional services or functions," as long as those services or functions are ones "for which the . . . institution would otherwise use employees," the outside party is "under the direct control of the . . . institution with respect to the use and maintenance of education records," and the outside party is subject to the same limitations as the institution on "the use and redisclosure of personally identifiable information from education records." 34 C.F.R. § 99.31(a)(1)(i)(B). A written contract is not required, but is advisable.

3. The disclosure is to another educational institution "where the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer." 34 C.F.R. § 99.31(a)(2). To take advantage of this exception, sometimes referred to as the "**transfer exception**," the disclosing institution must first give notice that it intends to respond to requests from other institutions for such information, either by making a "reasonable attempt" to notify the relevant students individually or – preferably – by informing all students generally in its annual notice. 34 C.F.R. § 99.34. Any prior school may disclose to the current or anticipated school under this exception, but the current or anticipated school may not use this exception to report back to prior schools.

4. The disclosure is **to the student** him- or herself. 34 C.F.R. § 99.31(a)(12).

5. The disclosure is to parents of a student who is considered their "**dependent**" for federal tax purposes. 34 C.F.R. § 99.31(a)(8). To establish the parents' eligibility to receive such a disclosure, the institution must obtain either a copy of the parents' most recent tax return (at least the first page, on which dependents are listed, but the financial portions of which the parents may redact) or an acknowledgment from the student that the student is, in fact, their dependent; the institution may not presume dependency. Note that because it is tied to the federal tax system, this exception generally is not available with respect to international students, whose parents generally do not file U.S. tax returns.

6. The disclosure is made "in connection with a **health or safety emergency**," is made only to "appropriate parties," and is limited to information that "is necessary to protect the health or safety of the student or other individuals." 34 C.F.R. §§ 99.31(a)(10) and 99.36. The institution has considerable discretion to determine for itself what situations constitute "emergencies," what parties are "appropriate," and what information is "necessary": "If, based on the information available at the time of the [institution's] determination, there is a rational basis for the determination, the Department will not substitute its judgment for that of the . . . institution." 34 C.F.R. § 99.36(c).

7. The disclosure is made to "comply with a **judicial order or lawfully issued subpoena**." 34 C.F.R. § 99.31(a)(9)(i). Before complying, the institution (or an outside contractor acting on its behalf pursuant to the "school official" exception) must in most cases first make a "reasonable effort to notify the . . . student of the order or subpoena in advance of compliance, so that the . . . student may seek protective action." 34 C.F.R. § 99.31(a)(9)(ii). The institution need not – and generally may not – give such advance notice in the case of grand jury or other law enforcement subpoenas, if the court or issuing agency has ordered that the existence or contents of the subpoena or information furnished in response not be disclosed, or in the case of *ex parte* court orders pursuant to the USA PATRIOT Act. Id. Note that the institution's obligations are limited to, at most, confirming the facial validity of the subpoena or order and notifying the student; it is not required to fight the order or subpoena on the student's behalf, and it may (and generally must) comply regardless of the student's wishes if the student fails to take action.

8. The disclosure is to a court in the context of a **lawsuit** that the student brought against the institution or that the institution brought against the student. 34 C.F.R. § 99.31(a)(9)(iii). The institution need not give the student advance notice of such a disclosure, but is limited to disclosing information that is "relevant" to the action and that does not relate to other students who are not adversary parties in the lawsuit. By interpretation, but not yet by regulation, the Family Policy Compliance Office has occasionally allowed an institution to make similar disclosures when one of its students has made a complaint to, or initiated some other form of adversary "proceeding" before, a government or similar agency having the power to take official action against the institution. *See*, *e.g.*, <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/library/cornell.html> Apart from these two limited instances, however, a student's disclosure of his or her own "education records" does not constitute an "implied waiver" of

FERPA rights that would justify further disclosures by the institution.

9. The disclosure is to parents of a student who is under the age of 21 *at the time of the disclosure* and relates to a determination by the institution that the student has violated its **drug or alcohol** rules. 34 C.F.R. § 99.31(a)(15).

10. The disclosure is of the "final results" of a disciplinary proceeding against a student whom the institution has determined violated an institutional rule or policy in connection with alleged acts that would, if proven, also constitute a "**crime of violence or non-forcible sex offense**." 34 C.F.R. § 99.31(a)(14). For purposes of this exception, "final results" is limited to the name of the student, the basic nature of the violation the student was found to have committed, and a description and the duration of any sanction the institution has imposed against the student. 34 C.F.R. § 99.39.

11. The disclosure is to "a **victim of an alleged perpetrator of a crime of violence or non-forcible sex offense**" and consists only of the "final results" (as defined above) of an institutional disciplinary proceeding in connection with that alleged crime or offense. The institution may (and, under the Campus Sexual Assault Victims' Bill of Rights Act, must upon request) make such a disclosure regardless of the outcome of the proceeding. 34 C.F.R. § 99.31(a)(13).

12. The disclosure is in connection with **financial aid** that the student has applied for or received and is for the purpose of determining the student's eligibility for, the amount of, or the conditions for the aid, or to enforce the terms and conditions of the aid. 34 C.F.R. § 99.31(a)(4).

13. The disclosure is to authorized representatives of the Comptroller General, Attorney General, Secretary of Education, or state or local educational authorities in connection with an **audit of federal- or state-supported education programs** or with the **enforcement of or compliance with federal legal requirements** relating to those programs. In the absence of consent or a specific federal law to the contrary, information collected under this exception must be protected so that individuals are not personally identifiable other than to the "authorized representatives," and the information must be destroyed when no longer needed. 34 C.F.R. §§ 99.31(a)(3) and 99.35. A recent, and controversial, reinterpretation of this provision now allows considerable sharing of information to and from state longitudinal database systems.

14. The disclosure is to **accrediting organizations** to carry out their accrediting functions. 34 C.F.R. § 99.31(a)(7).

15. The disclosure is to **organizations conducting studies** for educational institutions to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction, provided that the studies are conducted in a manner that prevents personal identification of parents and students by anyone other than representatives of the organizations, the information is destroyed when no longer needed for purposes of the studies, and the institution enters into a written agreement with the organization specifically limiting its use of the information in these ways. The institution need not initiate the study itself or agree with or endorse the study's conclusions. 34 C.F.R. § 99.31(a)(6). Moreover, under the recent reinterpretation noted above, state longitudinal database systems may conduct such studies for an institution even if the institution objects.

16. The disclosure concerns **sex offenders** and consists of information provided to the institution pursuant to the Violent Crime Control and Law Enforcement Act of 1994, commonly known as the "Wetterling Act." 34 C.F.R. § 99.31(a)(16).

Each of these exceptions is independent of the others. If you can find one that applies to your situation, it doesn't matter whether that situation also would qualify under any of the others. Thus, for example, if you have determined that a 19-year-old student's serious, alcohol-related injuries constitute a "health or safety emergency" that is "appropriate" to disclose to the student's parents, you need not also determine whether the student is their dependent for tax purposes or whether the student has violated your alcohol policies before making the disclosure.

Note also that, at least as far as FERPA itself is concerned, it is entirely within the institution's discretion whether to make a disclosure under any of these exceptions. 34 C.F.R. § 99.31(b). Thus, for example, a parent never has a *right*, under FERPA, to see his or her college student's education records, even if the student is the parent's dependent for tax purposes, is involved in a health or safety emergency, and has violated the institution's alcohol policies – and even if the student is not yet 18 years old. A subpoena, a court order, or another law such as the Campus Sexual Assault Victims' Bill of Rights Act may require broader disclosure in certain circumstances, but FERPA does not.

C. REDISCLOSURE

FERPA imposes similar limitations on redisclosure. In general, an institution disclosing personally identifiable information from an education record must inform the recipient that it cannot redisclose that information without the consent of the student and that it may use the information only for the purpose for which the disclosure was made. 34 C.F.R. § 99.33(a). Exceptions to this

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

D. RECORDKEEPING

The institution generally must maintain a record of each request for access to and each release of personally identifiable information from a student's education records. This separate record must include, at a minimum, the identities of the requesters and recipients and the "legitimate interests" they had in the information; in the case of a "health or safety emergency," it also must include a description of the perceived threat. In addition, it must be maintained with the student's education records for as long as those records are themselves maintained. 34 C.F.R. § 99.32(a). Exceptions to this requirement include disclosures to a school official, a parent or student, a person with written consent, or a person requesting directory information, and disclosures in connection with a grand jury or other law enforcement subpoena prohibiting disclosure of its existence or contents or an *ex parte* court order pursuant to the USA PATRIOT Act. 34 C.F.R. § 99.32(d).

IV. INSPECTION AND REVIEW

FERPA also gives college and university students the right to inspect and review their own education records. 34 C.F.R. § 99.10(a). The institution must provide access to the records within 45 days of a request and must respond to reasonable requests for explanations and interpretations of the records. 34 C.F.R. § 99.10(b) and (c). FERPA does *not* require the institution to provide copies of records to the student, unless "circumstances effectively prevent" the student from exercising the right to inspect and it is not possible to "make other arrangements" for inspection. 34 C.F.R. § 99.10(d). The institution may not destroy records while a request for their inspection is outstanding (but FERPA otherwise does not impose any records retention requirements). 34 C.F.R. § 99.10(e).

There are several limitations on the right of inspection. First, if the requested records contain information about more than one student, the requesting student may have access only to those portions pertaining to him- or herself. 34 C.F.R. § 99.12(a). (Note, however, that if information that is "directly related" to multiple students "cannot be segregated and redacted without destroying its meaning," each student may have access to the information even though it is also "directly related" to other students. 73 Fed. Reg. 74806, 74832-33 (Dec. 9, 2008).) In addition, students do not have the right to inspect the following:

1. Financial records of their parents. 34 C.F.R. § 99.12(b)(1).

2. Confidential letters and statements of recommendation, if the student has waived the right to review and inspect those documents and they are

related to the student's admission, application for employment, or receipt of an honor or honorary recognition. 34 C.F.R. § 99.12(b)(3). Such a waiver is valid only if it is not a condition of admission to or receipt of a benefit or service from the institution and it is in writing and signed by the student. 34 C.F.R. § 99.12(c)(1). If the student provides such a waiver, the student must be given, upon request, the names of the persons providing the recommendations, and the institution may not use the letters for any purpose other than that for which they were originally intended. 34 C.F.R. § 99.12(c)(2). The student may revoke the waiver in writing; however, revocation affects only those documents received after the date of the revocation. 34 C.F.R. § 99.12(c)(3). In other words, a student may not revoke the waiver in order to see documents already received.

3. "Treatment" records, as defined above in Section II. However, upon request, the student may have any such records reviewed by a physician or other appropriate professional of the student's choice. 34 C.F.R. § 99.10(f).

V. AMENDMENT

If a student believes that his or her education records contain inaccurate or misleading information or information that violates the student's right to privacy, the student may request that the institution amend the records. 34 C.F.R. § 99.20(a). The institution must make a decision on the request within a "reasonable time" after receipt. 34 C.F.R. § 99.20(b). If the institution decides not to make the requested amendment, it must so inform the student and advise the student of the right to a hearing. 34 C.F.R. § 99.20(c).

If the student requests a hearing, it must meet the following minimum requirements:

1. It must be held within a reasonable time after the request;

2. The student must be provided reasonable notice of the date, time, and place;

3. The individual conducting the hearing must not have a direct interest in the outcome;

4. The student must have a "full and fair opportunity" to present his or her case and may be assisted or represented by others, including an attorney; and

5. The decision must be in writing, rendered within a reasonable time after the hearing, and based solely on the evidence presented at the hearing, and it must include a summary of the evidence and the reasons for the decision.

34 C.F.R. § 99.22.

If, as a result of the hearing, the institution agrees with the student, it must amend the record and notify the student in writing. 34 C.F.R. § 99.21(b)(1). If the institution does not agree, it must advise the student that he or she may place a written statement in the file commenting on the contested information and/or stating the nature of the disagreement. 34 C.F.R. § 99.21(b)(2). If the student chooses this option, the statement must be maintained with the contested information and disclosed in conjunction with any subsequent release of the contested information. 34 C.F.R. § 99.21(c).

Both the Family Policy Compliance Office and the courts have ruled that this portion of FERPA is intended to deal with "scrivener's errors" in a record, not to provide a means by which a student may challenge the underlying substantive decisions that are recorded, such as grades, or obtain information on how a particular grade was assigned. *See*, *e.g.*, <http://www2.ed.gov/ policy/gen/guid/fpco/ferpa/library/parent.html>; *Adatsi v. Mathur*, 934 F.2d 910 (7th Cir. 1991) ("FERPA addresses the situation where a student seeks to have misleading or inaccurate information in his records corrected. There is nothing inaccurate about Adatsi's grade. He just feels he deserves something else. This fails to state a claim under FERPA."); *Tarka v. Cunningham*, 741 F. Supp. 1281, 1282 (W.D. Tex.), *aff'd*, 917 F.2d 890 (5th Cir. 1990) ("At most, a student is only entitled to know whether or not the assigned grade was recorded accurately in the student's record.").

VI. ANNUAL NOTIFICATION OF RIGHTS

FERPA requires each institution to notify its students annually of their rights under the act. 34 C.F.R. § 99.7. The best place to start (and perhaps end) is the Family Policy Compliance Office's model notice of rights, which is available at <http://www.ed.gov/policy/gen/guid/fpco/ferpa/ps-officials.html>. The notice may be provided by "any means that are reasonably likely to inform . . . students of their rights." 34 C.F.R. § 99.2(b). Each institution must also give "public notice" of its list of directory information and its procedure for "opting out." 34 C.F.R. § 99.37(a). The easiest way to do so is by including this information in the annual notice.

VII. ENFORCEMENT

The responsibility for enforcing FERPA rests with the Family Policy Compliance Office of the Department of Education, which is authorized to investigate and review potential violations and to provide technical assistance regarding compliance issues. 34 C.F.R. § 99.60. If it determines *both* that a complaint is meritorious *and* that the violation "was based on a policy or practice" rather than an isolated incident, the Office will recommend steps necessary to ensure compliance with the act and provide a reasonable time for the institution to come into compliance. 34 C.F.R. § 99.66(c). If – and only if – the institution does not come into compliance, the Department is then authorized to terminate all or any portion of the institution's federal funds or to take "any [other] legally available enforcement action." 34 C.F.R. § 99.67. In *Gonzaga University v. Doe*, 536 U.S. 273 (2002), the Supreme Court held that FERPA does not create personal rights that an individual may enforce through 42 U.S.C. § 1983.

VIII. RESOURCES

The Family Educational Rights and Privacy Act: A Legal Compendium (NACUA, 2d ed.)

William Kaplin and Barbara Lee, *The Law of Higher Education* (Jossey Bass, 4th ed.)

Family Policy Compliance Office: http://www.ed.gov/policy/gen/guid/fpco/index.html

Catholic University's FERPA Reference Chart:
http://counsel.cua.edu/ferpa/resources/recchart.cfm

University of Maryland's FERPA Tutorial: http://info.sis.usmd.edu/ferpaweb

AACRAO's FERPA Final Exam:
http://www.aacrao.org/Libraries/Compliance/FERPA_2010_Exam.sflb.ashx

Boston University's Policy Regarding Release of Information to Parents and Guardians:
http://www.bu.edu/reg/ferpa/ferpa-parent.html

Model Notification of Rights under FERPA for Postsecondary Institutions

The Family Educational Rights and Privacy Act (FERPA) afford eligible students certain rights with respect to their education records. (An "eligible student" under FERPA is a student who is 18 years of age or older or who attends a postsecondary institution.) These rights include:

1. The right to inspect and review the student's education records within 45 days after the day the [Name of postsecondary institution ("School")] receives a request for access. A student should submit to the registrar, dean, head of the academic department, or other appropriate official, a written request that identifies the record(s) the student wishes to inspect. The school official will make arrangements for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the school official to whom the request was submitted, that official shall advise the student of the correct official to whom the request should be addressed.

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

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

   If the school decides not to amend the record as requested, the school will notify the student in writing of the decision and the student's right to a hearing regarding the request for amendment. Additional information regarding the hearing procedures will be provided to the student when notified of the right to a hearing.

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

   The school discloses education records without a student's prior written consent under the FERPA exception for disclosure to school officials with legitimate educational interests. A school official is a person employed by the [School] in an administrative, supervisory, academic, research, or support staff position (including law enforcement unit personnel and health staff); a person serving on the board of trustees; or a student serving on an official committee, such as a disciplinary or grievance committee. A school official also may include a volunteer or contractor outside of the [School] who performs an institutional service of function for which the school would otherwise use its own employees and who is under the direct control of the school with respect to the use and maintenance of PII from education records, such as an attorney, auditor, or collection agent or a student volunteering to assist another school official in performing his or her tasks. A school official has a

legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibilities for the [School].

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

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

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

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

[Optional] See the list below of the disclosures that postsecondary institutions may make without consent.

FERPA permits the disclosure of PII from students' education records, without consent of the student, if the disclosure meets certain conditions found in §99.31 of the FERPA regulations. Except for disclosures to school officials, disclosures related to some judicial orders or lawfully issued subpoenas, disclosures of directory information, and disclosures to the student, §99.32 of FERPA regulations requires the institution to record the disclosure. Eligible students have a right to inspect and review the record of disclosures. A postsecondary institution may disclose PII from the education records without obtaining prior written consent of the student –

- To other school officials, including teachers, within the [School] whom the school has determined to have legitimate educational interests. This includes contractors, consultants, volunteers, or other parties to whom the school has outsourced institutional services or functions, provided that the conditions listed in §99.31(a)(1)(i)(B)(*1*) - (a)(1)(i)(B)(*2*) are met. (§99.31(a)(1))

- To officials of another school where the student seeks or intends to enroll, or where the student is already enrolled if the disclosure is for purposes related to the student's enrollment or transfer, subject to the requirements of §99.34. (§99.31(a)(2))

- To authorized representatives of the U. S. Comptroller General, the U. S. Attorney General, the U.S. Secretary of Education, or State and local educational authorities, such as a State postsecondary authority that is responsible for supervising the university's State-supported education programs. Disclosures under this provision may be made, subject to the requirements of §99.35, in connection with an audit or

evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. These entities may make further disclosures of PII to outside entities that are designated by them as their authorized representatives to conduct any audit, evaluation, or enforcement or compliance activity on their behalf. (§§99.31(a)(3) and 99.35)

- In connection with financial aid for which the student has applied or which the student has received, if the information is necessary to determine eligibility for the aid, determine the amount of the aid, determine the conditions of the aid, or enforce the terms and conditions of the aid. (§99.31(a)(4))

- To organizations conducting studies for, or on behalf of, the school, in order to: (a) develop, validate, or administer predictive tests; (b) administer student aid programs; or (c) improve instruction. (§99.31(a)(6))

- To accrediting organizations to carry out their accrediting functions. ((§99.31(a)(7))

- To parents of an eligible student if the student is a dependent for IRS tax purposes. (§99.31(a)(8))

- To comply with a judicial order or lawfully issued subpoena. (§99.31(a)(9))

- To appropriate officials in connection with a health or safety emergency, subject to §99.36. (§99.31(a)(10))

- Information the school has designated as "directory information" under §99.37. (§99.31(a)(11))

- To a victim of an alleged perpetrator of a crime of violence or a non-forcible sex offense, subject to the requirements of §99.39. The disclosure may only include the final results of the disciplinary proceeding with respect to that alleged crime or offense, regardless of the finding. (§99.31(a)(13))

- To the general public, the final results of a disciplinary proceeding, subject to the requirements of §99.39, if the school determines the student is an alleged perpetrator of a crime of violence or non-forcible sex offense and the student has committed a violation of the school's rules or policies with respect to the allegation made against him or her. (§99.31(a)(14))

- To parents of a student regarding the student's violation of any Federal, State, or local law, or of any rule or policy of the school, governing the use or possession of alcohol or a controlled substance if the school determines the student committed a disciplinary violation and the student is under the age of 21. (§99.31(a)(15))

Best Practices for Data Destruction

About PTAC

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems. More PTAC information is available on http://ptac.ed.gov.

PTAC welcomes input on this document and suggestions for future technical assistance resources relating to student privacy. Comments and suggestions can be sent to PrivacyTA@ed.gov.

Purpose

Educational agencies and institutions increasingly collect and maintain large amounts of data about students in order to provide educational services. Some data, like students' transcript information, may need to be preserved indefinitely. Other student information will need to be preserved for a prescribed period of time to comply with legal or policy requirements governing record retention, then will need to be destroyed once those time periods have elapsed. But a large amount of student information – some of which may still be highly sensitive – may become unnecessary or irrelevant the moment a student graduates or otherwise leaves the school, and can be destroyed immediately. Similarly, third parties providing services to a school or district, or conducting research or evaluations for a state or local educational agency, are often authorized to receive and use student data, but are typically required (either by law or by contract provisions) to destroy the student data when it is no longer needed for the specified purpose.

In most of these cases, merely deleting a digital record or file will be insufficient to destroy the information contained therein – as the underlying digital data are typically preserved in the system, and can often be "undeleted." Specific technical methods used to dispose of the data greatly impact the likelihood that any information might be recovered.

This document will provide an overview of various methods for disposing of electronic data, and will discuss how these methods relate to legal requirements and established best practices for protecting student information.

Legal Requirements

The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the confidentiality of student information. FERPA protects personally identifiable information (PII) from students' education records from disclosure without written consent from the parent or "eligible student" (a student who is 18 years of age, or who is attending a post-secondary institution), unless an exception to that consent requirement applies. For a detailed explanation of FERPA, the various exceptions to the consent requirement, and the requirements and conditions for each, please visit the PTAC website at http://ptac.ed.gov.

FERPA does not provide any specific requirements for educational agencies and institutions regarding disposition or destruction of the data they collect or maintain themselves, other than requiring them to safeguard FERPA-protected data from unauthorized disclosure, and not to destroy any education records if there is an outstanding request to inspect or review them. When educational agencies and institutions disclose (or "share") PII from education records with third parties under an applicable exception to FERPA's written consent requirement, however, additional legal requirements regarding destruction of that PII may apply.

Under the "school official" exception, FERPA requires that the school or district maintain direct control over the authorized recipient's maintenance and use of the PII from education records, and that the recipient protect the PII from further or unauthorized disclosure. While these general requirements for protection of and direct control over the maintenance of the PII imply adequate destruction of that PII when no longer needed, FERPA's school official exception leaves it to the educational agency or institution to establish specific terms for the protection of and direct control over the maintenance of the PII from education records (including its eventual destruction).

Two commonly used exceptions to FERPA's written consent requirement provide more specificity regarding data destruction. FERPA's "studies" and "audit or evaluation" exceptions require the disclosing agency or institution to enter into a written agreement with the third party receiving the PII from education records. Under these exceptions, the agreement must (among other things) specify that the PII must be destroyed when no longer needed for the specific purpose for which it was disclosed and a time period for that destruction. While FERPA does not provide any technical standards for destruction, the audit or evaluation exception does require that the disclosing entity use "reasonable methods" to ensure that the PII from education records is properly protected by the recipient. (For more information on these two exceptions, the other requirements for written agreements, or additional guidance on what constitutes "reasonable methods," visit the PTAC website at http://ptac.ed.gov).

While FERPA is silent on specific technical requirements governing data destruction, methods discussed in this document should be viewed as best practice recommendations for educational agencies and institutions to consider adopting when establishing record retention and data

governance policies to follow internally, and also for inclusion in any written agreements and contracts they make with third parties to whom they are disclosing PII.

It should also be noted that while FERPA does not require that particular methods of data destruction be used, other applicable Federal, State, or local privacy laws and regulations may require specific secure data disposal methods. When creating data sharing agreements, check with your legal counsel to fully understand what requirements apply and how to proceed.

Depending on the type of data involved and the context in which the data are being used, there may be a number of specific requirements with which educational agencies and institutions must comply. For example, Part B of the Individuals with Disabilities Education Act (IDEA) requires public agencies to inform a student's parents when any PII collected, maintained, or used thereunder is no longer needed to provide educational services to the child. Subsequently, the information must be destroyed at the request of the parents (though a permanent record of a student's name, address, and phone number, his or her grades, attendance record, classes attended, grade level completed, and year completed may be maintained without time limitation. 34 CFR § 300.624(a) and (b)). Part B of the IDEA defines the term "destruction" as the "physical destruction or removal of personal identifiers from information so that the information is no longer personally identifiable." 34 CFR § 300.611(a)

Lastly, methods discussed in this guidance are intended as examples and should not be considered to be exhaustive. More detailed technical information can be found in the National Institute of Standards and Technology (NIST) Special Publication 800-88 Rev. 1 (Draft): *Guidelines for Media Sanitization*.

What is Data Destruction?

Data should be appropriately managed across the entire data lifecycle, from capture to destruction. Planning for data destruction is an integral part of a high quality data management program.

Data in any of their forms move through stages during their useful life and ultimately are either archived for later use, or destroyed when their utility has been exhausted. Establishing policies and procedures governing the management and use of data allows an organization to more efficiently and

safely protect its data (see PTAC's resources on Data Governance at http://ptac.ed.gov). When data are no longer needed, the destruction of the data becomes a critical, and often required, component of an effective data governance program. Data destruction is the process of removing information in a way that renders it unreadable (for paper records) or irretrievable (for digital records).

Because some methods of data destruction are more complicated, time-consuming, or resource intensive than others, it is common to select the method based on the underlying sensitivity of the data being destroyed, or the potential harm they could cause if they are recovered or inadvertently disclosed. For very low risk information, this may mean simply deleting electronic files or using a desk shredder for paper documents. However, these types of destruction methods can be undone, by a determined and motivated individual, making these methods inappropriate for more sensitive data. For more sensitive data, stronger methods of destruction at a more granular level may need to be employed to assure that the data are truly irretrievable.

How Long Should Data Be Retained Before They Are Destroyed?

FERPA does not require educational agencies and institutions to destroy education records maintained as a part of the regular school or agency operations, and in fact, many jurisdictions require lengthy retention periods for student attendance and graduation records. For other student records, in order to minimize information technology (IT) costs and reduce the likelihood of inadvertent disclosure of student information, schools and districts will often elect to establish their own record retention policies, including time frames for eventual destruction of the records. Minimizing the amount of data you retain, by destroying them when no longer needed, is a key element of the Fair Information Practice Principles (FIPPs), and is widely considered to be a best practice for protecting individuals' privacy and for lessening the potential impact of a data breach or inadvertent disclosure. For more information on FIPPs (including Data Minimization), see http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

Under the "studies" and "audit or evaluation" exceptions, FERPA requires that PII from education records be destroyed when no longer needed for the specific purpose for which it was disclosed, and that the written agreement specify the time period for destruction. When drafting these agreements, it may be difficult to accurately predict the appropriate destruction period in advance. In these cases, the parties may wish to consider establishing a time period for destruction of the PII, and then modifying the written agreement, if needed, to postpone the destruction date or move it sooner than initially specified. This can be especially important for longitudinal studies, which may span many decades. While FERPA requires that there be an end date upon which any PII from education records disclosed under the studies or audit or evaluation exception must be destroyed, it does not specify a maximum time limit. In determining the appropriate time frame for the destruction of PII for a given study or audit or evaluation, some important issues should be considered. For example, for the purposes of verification and repeatability of findings, it may not be feasible to immediately destroy all of the PII involved in a study. In these cases, consider adding provisions within the agreement for the retention of PII needed for repeatability for an additional specified length of time. Additionally, an

educational agency or institution might consider using a strategy in which the third party returns the research dataset to the educational agency or institution for archiving. In these cases, the third party would then destroy residual PII, leaving the educational agency or institution with the study dataset.

Under the school official exception, it is a best practice for schools and districts to require the third party receiving the PII to destroy it upon termination of the school official relationship (e.g., when the contract ends), or when no longer needed for the purpose for which it was disclosed (whichever comes first).

When PII from education records is disclosed under any of FERPA's other exceptions, unless legal requirements specify otherwise, it is a best practice for educational agencies and institutions to require the recipient to destroy the PII when no longer needed for the purpose for which it was disclosed.

Please note that other Federal, state, and local privacy laws and regulations may contain more stringent data retention and/or destruction requirements, so it is important to consider and comply with all applicable requirements when determining the appropriate time period for retention and destruction of data.

Best Practices for Data Destruction

The information below contains some common best practices for data destruction. This guidance should not be considered comprehensive. Many additional technologies and methodologies exist which may or may not apply to your specific needs. While this document provides high level recommendations, the National Institute of Standards and Technology (NIST) provides in-depth guidance and best practices for the implementation of effective methods of data destruction in their *Guidelines for Media Sanitation*.

Modern electronic data storage devices are extremely resilient, and data recovery techniques and technology are highly advanced. Data are routinely recovered from media which have been burned, crushed, submerged in water, or impacted from great heights. In effect, it really is quite difficult to permanently get rid of data, but the permanent and irreversible destruction of data is a cornerstone of protecting the privacy and security of students' education records. Data destruction encompasses a wide variety of media, including electronic and paper records. The choice of destruction methodology should be based on the risk posed by the sensitivity of the data being destroyed and the potential impact of unauthorized disclosure. For example, the negative impact from the disclosure of a file containing directory information, such as names of honor roll students, might not be as severe as the negative impact from the disclosure of a file containing students' Social Security Numbers, names, and dates of birth. Therefore, the approach to data destruction in these two scenarios might be different. While the negative impact from the disclosure of de-identified data may warrant only their deletion from a disk or other media, the negative impact and risk of unauthorized disclosure of sensitive PII

typically would warrant stronger methods of data destruction. In the latter case, the organization might use a software or hardware technique that completely cleans the hard disk containing the PII to the point that the data cannot be retrieved, even forensically.

The table below identifies three major categories of data destruction. The table is arranged according to the degree of assurance each category provides, with "clear" providing the least amount of assurance and "destroy" providing the most assurance that the information is irretrievable. Organizations should make risk-based decisions on which method is most appropriate based on the data type, risk of disclosure, and the impact if that data were to be disclosed without authorization.

Data Destruction Categories

 **Clear**	**A method of sanitization that applies programmatic, software-based techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques; typically applied through the standard Read and Write commands to the storage device, such as by rewriting with a new value or using a menu option to reset the device to the factory state (where rewriting is not supported).**
 **Purge**	**A method of sanitization that applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.**
 **Destroy**	**A method of sanitization that renders Target Data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data.**

Adapted from NIST Draft Special Publication 800-88 Rev 1: Guidelines for Media Sanitization; Section 2.5 – Types of Sanitization

More information about the specific technical requirements for data destruction for various hardware and media types can be found in NIST's *Guidelines for Media Sanitation*, Appendix A: "Minimum Sanitization Recommendations."

No matter which method of destruction you choose, consider following these general best practices for data destruction:

- ✓ When drafting written agreements with third parties, include provisions that specify that all PII that was provided to the third party must be destroyed when no longer needed for the specific purpose for which it was provided, including any copies of the PII that may reside in system backups, temporary files, or other storage media.
- ✓ Ensure accountability for destruction of PII by using certification forms which are signed by the individual responsible for performing the destruction and contain detailed information about the destruction.
- ✓ Remember that PII may also be present in non-electronic media. Organizations should manage non-electronic records in a similar fashion to their electronic data. When data are no longer required, destroy non-electronic media using secure means to render it safe for disposal or recycling. Commonly used methods include cross-cut shredders, pulverizers, and incinerators.
- ✓ Depending on the sensitivity of the data being shared, be specific in the written agreement as to the type of destruction to be carried out.
- ✓ When destroying electronic data, use appropriate data deletion methods to ensure the data cannot be recovered. Please note that simple deletion of the data is not effective. Often, when a data file is deleted, only the reference to that file is removed from the media. The actual file data remain on the disk and are available for recovery until overwritten. Talk to your IT professional to ensure proper deletion of records consistent with technology best practice standards.
- ✓ Avoid using file deletion, disk formatting, and "one way" encryption to dispose of sensitive data—these methods are not effective because they leave the majority of the data intact and vulnerable to being retrieved by a determined person with the right tools.
- ✓ Destroy CDs, DVDs, and any magneto-optical disks by pulverizing, cross-cut shredding, or burning.
- ✓ Address in a timely manner sanitization of storage media which might have failed and need to be replaced under warranty or service contract. Many data breaches result from storage media containing sensitive information being returned to the manufacturer for service or replacement.
- ✓ Create formal, documented processes for data destruction within your organization and require that partner organizations do the same.

Best Practices in Data Destruction – An Example

A school district wants to evaluate how its former elementary students are doing in its high school to improve its elementary school instruction. The district decides to contract with a research organization to perform a study to determine ways to improve instruction in its elementary school.

The district enters into a written agreement with the research organization under the FERPA studies exception. The agreement establishes clear guidelines and data management requirements to protect the privacy and confidentiality of the data, specifying that:

- ✓ the study will take eight months to complete,
- ✓ the data provided by the district are to be used only for the express purposes outlined in the study,
- ✓ the research organization must put in place controls to limit access to the data and use secure file transfer process in accordance with the industry's standards for strong encryption mechanisms, and
- ✓ the data will be destroyed when no longer needed to conduct the study and by the end of the eight month contract.

In addition, the district stipulates in the written agreement that at the end of the contract the research dataset used for the study will be securely returned to the district, which will archive the file in case it is needed for future replication or evaluation of the findings, and that any remaining district data held by the research organization must be destroyed. The written agreement also stipulates the specific data destruction method that the research organization will use: in this case, a secure overwrite utility that overwrites the data files with random information, thus rendering the entirety of the data unrecoverable.

The written agreement explicitly identifies the person within the research organization who is responsible for the data while they are being used for the study, and the individual accountable for their destruction at the end of the project. The agreement also includes a destruction certification form on which the research organization must inventory the data destruction efforts, to be signed by the person responsible for destroying the data.

At the end of the contract, the research organization securely returns the study dataset back to the district and conducts the destruction of any remaining data using the agreed-upon tool to overwrite the data. The destruction is annotated on the form provided by the district and signed by the individual responsible for the destruction. The transport media that the district provided to the research organization for the purposes of conducting the study are securely returned to the district with the completed verification form.

Additional Resources

The resources below include links to federal regulations and several guidance documents outlining security issues, best practices and methodologies, and frameworks for secure data destruction.

- Family Policy Compliance Office, U.S. Department of Education, *Guidance for Reasonable Methods and Written Agreements* (2011): www.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf
- National Institute of Standards and Technology (NIST), *Guide for Conducting Risk Assessments*, *SP 800-30 Rev. 1* (2012): http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- National Institute of Standards and Technology (NIST), *Guidelines for Media Sanitization, Draft SP 800-88 Rev. 1* (2012): http://csrc.nist.gov/publications/drafts/800-88-rev1/sp800_88_r1_draft.pdf
- National Institute of Standards and Technology (NIST), *Guide to Selecting Information Technology Security Products* (2003): http://csrc.nist.gov/publications/nistpubs/800-36/NIST-SP800-36.pdf
- National Institute of Standards and Technology (NIST), *Standards for Security Categorization of Federal Information and Information Systems*, *Federal Information Processing Standards Publication (FIPS PUB) 199* (2004): http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- Privacy Technical Assistance Center (PTAC), U.S. Department of Education: http://ptac.ed.gov
- Privacy Technical Assistance Center, U.S. Department of Education, *Written Agreement Checklist* (2012): http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf
- U.S. Department of Education, *Family Educational Rights and Policy Act (FERPA) regulations amendment* (2011): www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf

Glossary

Education records means records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR § 99.3.

Encryption is the process of transforming information using a cryptographic algorithm (called a cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as an encryption/decryption key. "One way" encryption is a data destruction technique which makes use of encryption techniques to render data unusable by first encrypting the data and then destroying the key used to encrypt the data initially.

Personally identifiable information (PII) from education records includes information, such as a student's name or identification number, that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR § 99.3, for a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII.

Sanitization of the media is a process which is applied to data or storage media to make data retrieval unlikely for a given level of effort. *Clear*, *Purge*, and *Destroy* are actions that can be taken to sanitize data and media.

Sensitive data are data that carry the risk for adverse effects from an unauthorized or inadvertent disclosure. This includes any negative or unwanted effects experienced by an individual whose personally identifiable information (PII) from education records was the subject of a loss of confidentiality that may be socially, physically, or financially damaging, as well as any adverse effects experienced by the organization that maintains the PII. See *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, 2010, NIST Special Publication 800-122, for more information.

Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems and other uses of student data. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of student data systems. More PTAC information is available on http://ptac.ed.gov.

PTAC welcomes input on this document and suggestions for future technical assistance resources relating to student privacy. Comments and suggestions can be sent to PrivacyTA@ed.gov.

Purpose

Recent advances in technology and telecommunications have dramatically changed the landscape of education in the United States. Gone are the days when textbooks, photocopies, and filmstrips supplied the entirety of educational content to a classroom full of students. Today's classrooms increasingly employ on-demand delivery of personalized content, virtual forums for interacting with other students and teachers, and a wealth of other interactive technologies that help foster and enhance the learning process. Online forums help teachers share lesson plans; social media help students collaborate across classrooms; and web-based applications assist teachers in customizing the learning experience for each student to achieve greater learning outcomes.

Early adopters of these technologies have demonstrated their potential to transform the educational process, but they have also called attention to possible challenges. In particular, the information sharing, web-hosting, and telecommunication innovations that have enabled these new education technologies raise questions about how best to protect student privacy during use. This document will address a number of these questions, and present some requirements and best practices to consider, when evaluating the use of online educational services.

What are Online Educational Services?

This document will address privacy and security considerations relating to computer software, mobile applications (apps), and web-based tools provided by a third-party to a school or district that students and/or their parents access via the Internet and use as part of a school activity. Examples include online services that students use to access class readings, to view their learning progression, to watch

video demonstrations, to comment on class activities, or to complete their homework. This document does not address online services or social media that students may use in their personal capacity outside of school, nor does it apply to online services that a school or district may use to which students and/or their parents do not have access (e.g., an online student information system used exclusively by teachers and staff for administrative purposes).

Many different terms are used to describe both the online services discussed in this document (e.g., Ed Tech, educational web services, information and communications technology, etc.) and the companies and other organizations providing these services. This document will use the term "online educational services" to describe this broad category of tools and applications, and the term "provider" to describe the third-party vendors, contractors, and other service providers that make these services available to schools and districts.

Is Student Information Used in Online Educational Services Protected by FERPA?

It depends. Because of the diversity and variety of online educational services, there is no universal answer to this question. The Family Educational Rights and Privacy Act (FERPA) (see 20 U.S.C. § 1232g and 34 CFR Part 99) protects personally identifiable information (PII) from students' education records from unauthorized disclosure. FERPA defines education records as "records that are: (1) directly related to a student; and (2) maintained by an educational agency or institution or by a party acting for the agency or institution" (see 34 CFR § 99.3 definition of "education record"). FERPA also defines the term PII, which includes direct identifiers (such as a student's or other family member's name) and indirect identifiers (such as a student's date of birth, place of birth, or mother's maiden name) (see 34 CFR § 99.3 definition of "personally identifiable information"). For more information about FERPA, please visit the Family Policy Compliance Office's Web site at http://www.ed.gov/fpco.

Some types of online educational services do use FERPA-protected information. For example, a district may decide to use an online system to allow students (and their parents) to log in and access class materials. In order to create student accounts, the district or school will likely need to give the provider the students' names and contact information from the students' education records, which are protected by FERPA. Conversely, other types of online educational services may not implicate FERPA-protected information. For example, a teacher may have students watch video tutorials or complete interactive exercises offered by a provider that does not require individual students to log in. In these cases, no PII from the students' education records would be disclosed to (or maintained by) the provider.

Online educational services increasingly collect a large amount of contextual or transactional data as part of their operations, often referred to as "metadata." Metadata refer to information that provides meaning and context to other data being collected; for example, information about how long a particular student took to perform an online task has more meaning if the user knows the date and time when the student completed the activity, how many attempts the student made, and how long the student's mouse hovered over an item (potentially indicating indecision).

Metadata that have been stripped of all direct and indirect identifiers are not considered protected information under FERPA because they are not PII. A provider that has been granted access to PII from education records under the school official exception may use any metadata that are not linked to FERPA-protected information for other purposes, unless otherwise prohibited by the terms of their agreement with the school or district.

Schools and districts will typically need to evaluate the use of online educational services on a case-by-case basis to determine if FERPA-protected information (i.e., PII from education records) is implicated. If so, schools and districts must ensure that FERPA requirements are met (as well as the requirements of any other applicable federal, state, tribal, or local laws).

EXAMPLE 1: A district enters into an agreement to use an online tutoring and teaching program and discloses PII from education records needed to establish accounts for individual students using FERPA's school official exception. The provider sends reports on student progress to teachers on a weekly basis, summarizing how each student is progressing. The provider collects metadata about student activity, including time spent online, desktop vs. mobile access, success rates, and keystroke information. If the provider de-identifies these metadata by removing all direct and indirect identifying information about the individual students (including school and most geographic information), the provider can then use this information to develop new personalized learning products and services (unless the district's agreement with the provider precludes this use).

What Does FERPA Require if PII from Students' Education Records is Disclosed to a Provider?

It depends. Because of the diversity and variety of online educational services, there is no universal answer to this question. Subject to exceptions, the general rule under FERPA is that a school or district cannot disclose PII from education records to a provider unless the school or district has first obtained written consent from the parents (or from "eligible students," i.e., those who are 18 years of age or older or attending a postsecondary school). Accordingly, schools and districts must either obtain consent, or ensure that the arrangement with the provider meets one of FERPA's exceptions to the written consent requirement.

While disclosures of PII to create user accounts or to set up individual student profiles may be accomplished under the "directory information" exception, more frequently this type of disclosure will be made under FERPA's school official exception. "Directory information" is information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed (see 34 CFR § 99.3 definition of "directory information"). Typical examples of directory information include student name and address. To disclose student information under this exception, individual school districts must establish the specific elements or categories of directory information that they intend to disclose and publish those elements or categories in a public notice. While the directory information exception can seem to be an easy way to share PII from education

records with providers, this approach may be insufficient for several reasons. First, only information specifically identified as directory information in the school's or district's public notice may be disclosed under this exception. Furthermore, parents (and eligible students) generally have the right to "opt out" of disclosures under this exception, thereby precluding the sharing of information about those students with providers. Given the number of parents (and eligible students) who elect to opt out of directory information, schools and districts may not find this exception feasible for disclosing PII from education records to providers to create student accounts or profiles.

The FERPA school official exception is more likely to apply to schools' and districts' use of online educational services. Under the school official exception, schools and districts may disclose PII from students' education records to a provider as long as the provider:

1. Performs an institutional service or function for which the school or district would otherwise use its own employees;

2. Has been determined to meet the criteria set forth in in the school's or district's annual notification of FERPA rights for being a school official with a legitimate educational interest in the education records;

3. Is under the direct control of the school or district with regard to the use and maintenance of education records; and

4. Uses education records only for authorized purposes and may not re-disclose PII from education records to other parties (unless the provider has specific authorization from the school or district to do so and it is otherwise permitted by FERPA).

See 34 CFR § 99.31(a)(1)(i).

Two of these requirements are of particular importance. First, the provider of the service receiving the PII must have been determined to meet the criteria for being a school official with a "legitimate educational interest" as set forth in the school's or district's annual FERPA notification. Second, the framework under which the school or district uses the service must satisfy the "direct control" requirement by restricting the provider from using the PII for unauthorized purposes. While FERPA regulations do not require a written agreement for use in disclosures under the school official exception, in practice, schools and districts wishing to outsource services will usually be able to establish direct control through a contract signed by both the school or district and the provider. In some cases, the "Terms of Service" (TOS) agreed to by the school or district, prior to using the online educational services, may contain all of the necessary legal provisions governing access, use, and protection of the data, and thus may be sufficient to legally bind the provider to terms that are consistent with these direct control requirements.

When disclosing PII from education records to providers under the school official exception, schools and districts should be mindful of FERPA's provisions governing parents' (and eligible students') access to the students' education records. Whenever a provider maintains a student's education records, the

school and district must be able to provide the requesting parent (or eligible student) with access to those records. Schools and districts should ensure that their agreements with providers include provisions to allow for direct or indirect parental access. Under FERPA, a school must comply with a request from a parent or eligible student for access to education records within a reasonable period of time, but not more than 45 days after it has received the request. Some States have laws that require access to education records sooner than 45 days.

Schools and districts are encouraged to remember that FERPA represents a minimum set of requirements to follow. Thus, even when sharing PII from education records under an exception to FERPA's consent requirement, it is considered a best practice to adopt a comprehensive approach to protecting student privacy when using online educational services.

Do FERPA and the Protection of Pupil Rights Amendment (PPRA) Limit What Providers Can Do with the Student Information They Collect or Receive?

On occasion, providers may seek to use the student information they receive or collect through online educational services for other purposes than that for which they received the information, like marketing new products or services to the student, targeting individual students with directed advertisements, or selling the information to a third party. If the school or district has shared information under FERPA's school official exception, however, the provider cannot use the FERPA-protected information for any other purpose than the purpose for which it was disclosed.

Any PII from students' education records that the provider receives under FERPA's school official exception may only be used for the specific purpose for which it was disclosed (i.e., to perform the outsourced institutional service or function, and the school or district must have direct control over the use and maintenance of the PII by the provider receiving the PII). Further, under FERPA's school official exception, the provider may not share (or sell) FERPA-protected information, or re-use it for any other purposes, except as directed by the school or district and as permitted by FERPA.

It is important to remember, however, that student information that has been properly de-identified or that is shared under the "directory information" exception, is not protected by FERPA, and thus is not subject to FERPA's use and re-disclosure limitations.

EXAMPLE 2: A district contracts with a provider to manage its cafeteria account services. Using the school official exception, the district gives the provider student names and other information from school records (not just directory information). The provider sets up an online system that allows the school, parents, and students to access cafeteria information to verify account balances and review the students' meal selections. The provider cannot sell the student roster to a third party, nor can it use PII from education records to target students for advertisements for foods that they often purchase at school under FERPA because the provider would then be using FERPA-protected information for different purposes than those for which the information was shared.

FERPA is not the only statute that limits what providers can do with student information. The Protection of Pupil Rights Amendment (PPRA) provides parents with certain rights with regard to some marketing activities in schools. Specifically, PPRA requires that a school district must, with exceptions, directly notify parents of students who are scheduled to participate in activities involving the collection, disclosure, or use of personal information collected from students for marketing purposes, or to sell or otherwise provide that information to others for marketing purposes, and to give parents the opportunity to opt-out of these activities. 20 U.S.C. § 1232h(c)(2)(C)(i). Subject to the same exceptions, PPRA also requires districts to develop and adopt policies, in consultation with parents, about these activities. 20 U.S.C. § 1232h(c)(1)(E) and (c)(4)(A). PPRA has an important exception, however, as neither parental notice and the opportunity to opt-out nor the development and adoption of policies are required for school districts to use students' personal information that they collect from students for the exclusive purpose of developing, evaluating, or providing educational products or services for students or schools. 20 U.S.C. § 1232h(c)(4)(A).

While FERPA protects PII from education records maintained by a school or district, PPRA is invoked when personal information is collected from the student. The use of online educational services may give rise to situations where the school or district provides FERPA-protected data to open accounts for students, and subsequent information gathered through the student's interaction with the online educational service may implicate PPRA. Student information collected or maintained as part of an online educational service may be protected under FERPA, under PPRA, under both statutes, or not protected by either. Which statute applies depends on the content of the information, how it is collected or disclosed, and the purposes for which it is used.

It is important to remember that even though PPRA only applies to K-12 institutions, there is no time-limit on the limitations governing the use of personal information collected from students for marketing purposes. So, for example, while PPRA would not limit the use of information collected from college students for marketing, it would restrict the use of information collected from students while they were still in high school (if no notice or opportunity to opt-out was provided) even after those students graduate.

EXAMPLE 3: A district contracts with an online tutoring service using the school official exception. As part of the service, the provider uses data about individual students to personalize learning modules for the district's students. This does not implicate the PPRA because the activity falls under the PPRA exception for educational services and products. This use of data about individual students is similarly permissible under FERPA because the provider is only using any FERPA-protected information for the purposes for which it was shared.

EXAMPLE 4: A district contracts under the school official exception with a provider for basic productivity applications to help educate students: email, calendaring, web-search, and document collaboration software. The district sets up the user accounts, using basic enrollment information (name, grade, etc.) from student records. Under FERPA, the provider may not use data about individual student preferences gleaned from scanning student content to target ads to individual students for clothing or toys, because using the data for these purposes was not authorized by the district and does not constitute a legitimate educational interest as specified in the district's annual notification of FERPA rights.

PPRA would similarly prohibit targeted ads for clothing or toys, unless the district had a policy addressing this and parents were notified and given the opportunity to opt-out of such marketing. In spite of these limitations, however, the provider may use data (even in individually identifiable form) to improve its delivery of these applications, including spam filtering and usage monitoring. The provider may also use any non-PII data, such as metadata with all direct and indirect identifiers removed, to create new products and services that the provider could market to schools and districts.

Schools and districts should be aware that neither FERPA nor the PPRA absolutely prohibits them from allowing providers to serve generalized, non-targeted advertisements. FERPA would not prohibit, for example, a school from selling space on billboards on the football field, nor would it prohibit a school or district from allowing a provider acting as a school official from serving ads to all students in email or other online services.

Finally, schools and districts should remember their important role in setting policies to protect student privacy. While FERPA and PPRA provide important protections for student information, additional use or disclosure restrictions may be advisable depending on the situation and the sensitivity of the information. Any additional protections that a school or district would like to require should be documented in the written agreement (the contract or TOS) with the provider.

What are Some Other Best Practices for Protecting Student Privacy When Using Online Educational Services?

Regardless of whether FERPA or PPRA applies to a school's or district's proposed use of online educational services, the Department recommends that schools and districts follow privacy, security, and transparency best practices, such as:

- **Maintain awareness of other relevant federal, state, tribal, or local laws.**

  FERPA and PPRA are not the only laws that protect student information. Other federal, state, tribal, or local laws may apply to online educational services, and may limit the information that can be shared with providers. In particular, schools and districts should be aware of and

consider the requirements of the Children's Online Privacy and Protection Act (COPPA) before using online educational services for children under age 13. In general, COPPA applies to commercial Web sites and online services directed to children and those Web sites and services with actual knowledge that they have collected personal information from children. Absent an exception, these sites must obtain verifiable parental consent prior to collecting personal information from children. The Federal Trade Commission (FTC) has interpreted COPPA to allow schools to exercise consent on behalf of parents in certain, limited circumstances (see http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools).

- **Be aware of which online educational services are currently being used in your district.**

  Conduct an inventory of the online educational services currently being used within your school or district. Not only will this help assess the scope and range of student information being shared with providers, but having a master list of online educational services will help school officials to collaboratively evaluate which services are most effective, and help foster informed communication with parents.

- **Have policies and procedures to evaluate and approve proposed online educational services**.

  Establish and enforce school and district-wide policies for evaluating and approving online educational services prior to implementation. Schools and districts should be clear with both teachers and administrators about how proposed online educational services can be approved, and who has the authority to enter into agreements with providers. This is true not only for formal contracts, but also for consumer-oriented "Click-Wrap" software that is acquired simply by clicking "accept" to the provider's TOS. With Click-Wrap agreements, the act of clicking a button to accept the TOS serves to enter the provider and the end-user (in this case, the school or district) into a contractual relationship akin to signing a contract.

  Most schools or districts already have processes in place for evaluating vendor contracts for privacy and security considerations; using these established procedures may be the most effective way to evaluate proposed online educational services. It is particularly important that teachers and staff not bypass internal controls in the acquisition process when deciding to use free online educational services. To ensure that privacy and security concerns relating to these free services are adequately considered, the Department recommends that free online educational services go through the same (or a similar) approval process as paid educational services to ensure that they do not present a risk to the privacy or security of students' data or to the schools and district's IT systems. Following standard internal controls, including testing, will also enable the schools and district's IT personnel to assist in the implementation process. Simple and more streamlined processes will, of course, generate greater compliance.

- **When possible, use a written contract or legal agreement.**

  As mentioned above, the use of online educational services usually involves some form of a

contract or legal agreement between the school and the provider. Having a written contract or legal agreement helps schools and districts maintain the required "direct control" over the use and maintenance of student data. Even when FERPA is not implicated, the Department recommends using written agreements as a best practice. When drafting and reviewing these contracts, the Department recommends the inclusion of certain provisions:

- Security and Data Stewardship Provisions. Make clear whether the data collected belongs to the school/district or the provider, describe each party's responsibilities in the event of a data breach (see PTAC's Data Breach Response Checklist), and, when appropriate, establish minimum security controls that must be met and allow for a security audit.

- Collection Provisions. Be specific about the information the provider will collect (e.g., forms, logs, cookies, tracking pixels, etc.).

- Data Use, Retention, Disclosure, and Destruction Provisions. Define the specific purposes for which the provider may use student information, and bind the provider to only those approved uses. If student information is being shared under the school official exception to consent in FERPA, then it would also be a best practice to specify in the agreement how the school or district will be exercising "direct control" over the third party provider's use and maintenance of the data. Specify with whom the provider may share (re-disclose) student information, and if PII from students' education records is involved, ensure that these provisions are consistent with FERPA. Include data archival and destruction requirements to ensure student information is no longer residing on the provider's systems after the contract period is complete. When appropriate, define what disclosure avoidance procedures must be performed to de-identify student information before the provider may retain it, share it with other parties, or use it for other purposes.

- Data Access Provisions. Specify whether the school, district and/or parents (or eligible students) will be permitted to access the data (and if so, to which data) and explain the process for obtaining access. This is especially important if the online educational services will be creating new education records that will be maintained by the provider on behalf of the school or district, as FERPA's requirements regarding parental (or eligible students') access will then apply. To avoid the challenges involved in proper authentication of students' parents by the provider, the Department recommends that the school or district serve as the intermediary for these requests, wherein the parent requests access to any education records created and maintained by the provider directly from the school or district, and the school or district then obtains the records from the provider to give back to the parent.

- Modification, Duration, and Termination Provisions. Establish how long the agreement will be in force, what the procedures will be for modifying the terms of the agreement

(mutual consent to any changes is a best practice), and what both parties' responsibilities will be upon termination of the agreement, particularly regarding disposition of student information maintained by the provider.

- Indemnification and Warranty Provisions. Carefully assess the need for and legality of any such provisions and determine whether applicable state or tribal law prohibits or limits the school's or district's ability to indemnify a provider. Analyze whether there should be indemnification provisions in which the provider agrees to indemnify the school or district, particularly relating to a school's or district's potential liabilities resulting from a provider's failure to comply with applicable federal, state, or tribal laws. Given that the Department looks to schools and districts to comply with FERPA and PPRA, be specific about what you will require the provider to do in order to comply with applicable state and federal laws, such as FERPA and PPRA, and what the provider agrees to do to remedy a violation of these requirements and compensate the school or district for damages resulting from the provider's violation.

- **Extra steps are necessary when accepting Click-Wrap licenses for consumer apps.**

  Schools and districts sometimes can't negotiate agreements with providers of consumer apps, and are faced with a choice to accept the providers' TOS or not use the app. Extra caution and extra steps are warranted before employing Click-Wrap consumer apps:

  - Check Amendment Provisions. In addition to reviewing for the above terms, you should review the TOS to determine if the provider has retained the right to amend the TOS without notice. If the provider will be using FERPA-protected information, schools and districts should exercise caution when entering into Click-Wrap agreements that allow for amendment without notice, given FERPA's requirement to maintain "direct control" over the use and maintenance of the information under the school official exception. It is a best practice to review these agreements regularly to determine if any provisions have changed, and if so, to re-evaluate whether to continue using the service.

  - Print or Save the TOS. When accepting a Click-Wrap agreement, you should save a copy of the TOS that you have agreed to. You can either download and save a digital copy, or print and file a copy.

  - Limit Authority to Accept TOS. One potential issue with Click-Wrap agreements is that they can be easily accepted, without going through normal district or school approval channels. Individual teachers may not understand the specifics of how the provider will use and secure student data. Districts or schools should develop policies outlining when individual teachers may download and use Click-Wrap software.

EXAMPLE 5: A teacher who has many remote students wants to foster increased collaboration and socialization among her students. Pursuant to her district's policy, she selects a service from a district-approved list of providers, and accepts the provider's Click-Wrap agreement before creating the user accounts for all students (including those who opted out of directory information). Her students successfully participate in a students-only social collaboration space.

EXAMPLE 6: A teacher wants students to be able to share photographs and videos online and identifies an app that will allow this sharing. He creates user accounts for all students (including those who opted out of directory information) and accepts the app's Click-Wrap agreement without reading it. The TOS allow the provider to use the information for a variety of non-educational purposes, including selling merchandise. The district discovers that this service is being used and determines that the TOS violate FERPA. The district proceeds to block access to the service from district computers, and begins negotiations with the provider to delete the user accounts and any information attached to them.

- **Be transparent with parents and students.**

  The Department encourages schools and districts to be as transparent as possible with parents and students about how the school or district collects, shares, protects, and uses student data. FERPA requires that schools and districts issue an annual notification to parents and eligible students explaining their rights under FERPA (34 CFR § 99.7), and many schools and districts elect to combine their directory information policy public notice, required pursuant to §99.37 of the regulations, with their annual notice of rights. PPRA also requires schools and districts to provide parents and students with effective notice of their PPRA rights, to provide notice to parents of district policies (developed and adopted in consultation with parents) regarding specific activities, and to notify them of the dates of specific events and the opportunity to opt out of participating in those events. Beyond FERPA and PPRA compliance, however, the Department recommends that schools and districts clearly explain on their Web sites how and with whom they share student data, and that they post any school and district policies on outsourcing of school functions, including online educational services. Schools and districts may also want to post copies of the privacy and security provisions of important third party contracts.

  With online educational services, it can often be unclear what information is being collected while students are using the technology. Even when this information is not protected by FERPA or other privacy laws, it is a best practice to inform students and their parents of what information is being collected and how it will be used. When appropriate, the Department recommends that schools or districts develop an education technology plan that addresses student privacy and information security issues, and solicit feedback from parents about the plan prior to its implementation or the adoption of new online education services.

Transparency provides parents, students, and the general public with important information about how the school or district protects the privacy of student data. Greater transparency enables parents, students, and the public to develop informed opinions about the benefits and risks of using education technology and helps alleviate confusion and misunderstandings about what data will be shared and how they will be used.

- **Consider that parental consent may be appropriate.**

  Even in instances where FERPA does not require parental consent, schools and districts should consider whether consent is appropriate. These are individual determinations that should be made on a case-by-case basis.

Additional Resources

Materials below include links to resources that provide additional best practice recommendations and guidance relating to use of online educational services. Please note that these resources do not necessarily address the particular legal requirements, including FERPA, that your school and district need to meet when collecting, storing, disseminating, or releasing education records to a provider. It is always a best practice to consult legal counsel to determine the applicable federal, state, tribal, and local requirements prior to entering into contractual agreements with providers. Some resources prepared by third-party experts are included as well.

- Family Policy Compliance Office, U.S. Department of Education, *Model Notice for Directory Information:* *http://www.ed.gov/policy/gen/guid/fpco/ferpa/mndirectoryinfo.html*
- National Institute of Standards and Technology, Computer Security Resource Center: http://csrc.nist.gov/publications/
- National Institute of Standards and Technology, *Guidelines on Security and Privacy in Public Cloud Computing* (2011): http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf
- National Institute of Standards and Technology, *Standards for Security Categorization of Federal Information and Information Systems, Federal Information Processing Standards Publications (FIPS) 199* (2004): http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- Privacy Technical Assistance Center, U.S. Department of Education: http://ptac.ed.gov
- Privacy Technical Assistance Center, U.S. Department of Education, *Checklist – Data Breach Response* (2012): http://ptac.ed.gov/sites/default/files/checklist_data_breach_response_092012.pdf
- Privacy Technical Assistance Center, U.S. Department of Education, *Written Agreement Checklist* (2012): http://ptac.ed.gov/sites/default/files/data-sharing-agreement-checklist.pdf
- U.S. Federal Trade Commission, *Complying with COPPA: Frequently Asked Questions - COPPA AND SCHOOLS* (2013): http://www.business.ftc.gov/documents/Complying-with-COPPA-Frequently-Asked-Questions#Schools
- U.S. Federal Trade Commission, *FTC Strengthens Kid's Privacy, Gives Parents Greater Control Over Their Information By Amending Children's Online Protection Rule* (2012): http://www.ftc.gov/opa/2012/12/coppa.shtm

Glossary

Directory Information is information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. Typically, "directory information" includes information such as name, address, telephone listing, date and place of birth, participation in officially recognized activities and sports, and dates of attendance. A school may disclose "directory information" to third parties without consent if it has given public notice of the types of information which it has designated as "directory information," the parent's or eligible student's right to restrict the disclosure of such information, and the period of time within which a parent or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as "directory information." 34 CFR § 99.3 and 34 CFR § 99.37.

Education records means records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations. 34 CFR § 99.3.

Eligible Student means a student to whom FERPA rights have transferred upon turning 18 years of age, or upon enrolling in a post-secondary institution at any age. 34 CFR § 99.3.

Personally identifiable information (PII) is a FERPA term referring to identifiable information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR § 99.3, for a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII.

Personal Information Collected from Students is a PPRA term referring to individually identifiable information including a student or parent's first and last name; a home or other physical address (including street name and the name of the city or town); a telephone number; or a Social Security identification number collected from any elementary or secondary school student. 20 U.S.C. § 1232h(c)(6)(E).

School Official means any employee, including teacher, that the school or district has determined to have a "legitimate educational interest" in the personally identifiable information from an education record of a student. School officials may also include third party contractors, consultants, volunteers, service providers, or other party with whom the school or district has outsourced institutional services or functions for which the school or district would otherwise use employees under the school official exception in FERPA. 34 CFR § 99.31(a)(1).

Applied FERPA: Campus Safety and Discipline

Note: The following pages consist of excerpts of the following documents issued by the U.S. Department of Education. We have provided only those pages that address the intersection of FERPA and student disciplinary proceedings. The complete documents can be accessed by clicking on the links provided below.

Intersection of Title IX and the Clery Act (chart) (April 29, 2014)

Questions and Answers on Title IX and Sexual Violence (April 29, 2014)

Dear Colleague Letter: Sexual Violence (April 4, 2011)

Revised Sexual Harassment Guidance: Harassment of Students by School Employees, Other Students, or Third Parties (January 2001)

Intersection of Title IX and the Clery Act

The purpose of this chart is to clarify the reporting requirements of Title IX and the Clery Act in cases of sexual violence and to resolve any concerns about apparent conflicts between the two laws. To date, the Department of Education has not identified any specific conflicts between Title IX and the Clery Act.

Title IX	The Clery Act
What types of incidents must be reported to school officials under Title IX and the Clery Act?	
Overview: Title IX promotes equal opportunity by providing that no person may be subjected to discrimination on the basis of sex under any educational program or activity receiving federal financial assistance. A school must respond promptly and effectively to sexual harassment, including sexual violence, that creates a hostile environment. When responsible employees know or should know about possible sexual harassment or sexual violence they must report it to the Title IX coordinator or other school designee. ➢ **Sexual Harassment:** Sexual harassment is unwelcome conduct of a sexual nature, including unwelcome sexual advances, requests for sexual favors, and other verbal, nonverbal, or physical conduct of a sexual nature. ➢ **Sexual Violence:** Sexual violence is a form of sexual harassment. Sexual violence refers to physical sexual acts perpetrated against a person's will or where a person is incapable of giving consent (*e.g.*, due to the student's age or use of drugs or alcohol or an intellectual or other disability that prevents the student from having the capacity to give consent). Sexual violence includes rape, sexual assault, sexual battery, sexual abuse, and sexual coercion.	**Overview:** The Clery Act promotes campus safety by ensuring that students, employees, parents, and the broader community are well-informed about important public safety and crime prevention matters. Institutions that receive Title IV funds must disclose accurate and complete crime statistics for incidents that are reported to Campus Security Authorities (CSAs) and local law enforcement as having occurred on or near the campus. Schools must also disclose campus safety policies and procedures that specifically address topic such as sexual assault prevention, drug and alcohol abuse prevention, and emergency response and evacuation. The Clery Act also promotes transparency and ongoing communication about campus crimes and other threats to health and safety and empowers members to take a more active role in their own safety and security. **Criminal Offenses:** Criminal homicide; rape and other sexual assaults; robbery; aggravated assault; burglary; motor vehicle theft; and, arson as well as arrests and disciplinary referrals for violations of drug, liquor, and weapons laws. ➢ **Hate Crimes:** Any of the above-mentioned offenses against persons and property and incidents of larceny-theft, simple assault, intimidation or destruction/damage/vandalism of property, in which an individual or group is intentionally targeted because of their actual or perceived race, gender, religion, national origin, sexual orientation, gender identity, ethnicity, or disability. 20 U.S.C. §1092(f)(1)(F)(ii). Use FBI definitions, and the

Aggregate Data ➢ In order to identify patterns or systemic problems related to sexual violence, a school should collect aggregate data about sexual violence incidents from non-professional counselors or advocates in their on-campus sexual assault centers, victim advocacy offices, women's centers, or health centers. ➢ Such individuals should report only general information about incidents of sexual violence such as the nature, date, time, and general location of the incident and should take care to avoid reporting information that would personally identify a student. Non-professional counselors and advocates should consult with students regarding what information needs to be withheld to protect their identity.	**Aggregate Data** ➢ Typically, most non-law enforcement/campus safety officer CSAs must only report the nature, date, time, general location, and the current disposition of the incident, if known. ➢ Most non-law enforcement/campus safety officer CSAs typically are not required to disclose PII or other information that would have the effect of identifying the victim.

What must a school tell the complainant about the outcome of a sexual violence complaint and how does FERPA apply?[1]

Notice of the Outcome ➢ Title IX requires a school to tell the complainant whether or not it found that the sexual violence occurred, any individual remedies offered or provided to the complainant or any sanctions imposed on the perpetrator that directly relate to the complainant, and other steps the school has taken to eliminate the hostile environment, and prevent recurrence. ➢ Sanctions that directly relate to the complainant include, but are not limited to, requiring that the perpetrator stay away from the complainant until both parties graduate, prohibiting the perpetrator from attending	**Results of Institutional Disciplinary Proceedings** ➢ The Clery Act specifically mandates that "each institution shall develop and distribute procedures for simultaneously notifying the accuser and accused of the outcome of institutional disciplinary proceedings." 20 U.S.C. §485f(1)(J)(8)(B)(iv)(III)(aa). ➢ FERPA includes a provision that specifically allows schools to disclose to alleged victims of any crime of violence or rape and other sexual assaults, the final results of any disciplinary proceedings conducted by the institution against the alleged perpetrator of the offense. 20 U.S.C.

[1] This chart also addresses how the Family Educational Rights and Privacy Act (FERPA) applies to Title IX and the Clery Act. Once again, the Department of Education has not identified any specific situations where compliance with Title IX or the Clery Act will cause an institution to violate FERPA.

school for a period of time or transferring the perpetrator to another residence hall, other classes, or another school.

- The Department of Education interprets FERPA as not conflicting with the Title IX requirement that the school notify the complainant of the outcome of its investigation, *i.e.*, whether or not the sexual violence was found to have occurred, because this information directly relates to the victim. FERPA also permits the school to notify a complainant of sanctions imposed upon a student who was found to have engaged in sexual violence when the sanction directly relates to the complainant.
- The FERPA limits on re-disclosure of information do not apply to information that institutions are required to disclose under the Clery Act. 34 C.F.R. §99.33(c). Institutions may not require a complainant to abide by a nondisclosure agreement, in writing, or otherwise, that would prevent the re-disclosure of this information in any Title IX complaint that involves a Clery Act offense, such as sexual violence.

§1232g(b)(6).

- The "final results" of any proceeding are defined as: the name of the student, the findings of the proceeding board/official, any sanctions imposed by the institution, and the rationale for the findings and sanctions (if any). The presence of names of any other student, such as a victim or witnesses, may be included only with the consent of that student. 20 U.S.C. §1232g(c).
- The FERPA limits on re-disclosure of information do not apply to information that institutions are required to disclose under the Clery Act. 34 C.F.R. §99.33(c). Institutions may not require a complainant to abide by a nondisclosure agreement, in writing, or otherwise, that would prevent the re-disclosure of this information.

How does FERPA apply to other obligations under Title IX and the Clery Act?

All Other Title IX Obligations

- FERPA continues to apply in the context of Title IX enforcement, but if there is a direct conflict between the requirements of FERPA and the requirements of Title IX, such that enforcement of FERPA would interfere with the primary purpose of Title IX to eliminate sex-based discrimination in schools, the requirements of Title IX override any conflicting FERPA provisions.

Timely Warnings

- The Clery Act requires institutions to issue timely warnings to the campus community about crimes that have already occurred but may continue to pose a serious or ongoing threat to students and employees. Timely warnings are only required for Clery-reportable crimes that occur on Clery Geography although institutions are encouraged to issue appropriate warnings regarding other criminal activity that may pose a serious threat as well. 20 U.S.C. §485f(1)(J)(3); Handbook, 118.
- FERPA does not preclude an institution's compliance with the timely warning provision of the Clery Act. FERPA recognizes that information can, in the case of an emergency, be released without consent when needed to protect the health and safety of others. 34 C.F.R. §99.36(a). Further, if

	institutions utilize information from the records of campus law enforcement to issue a timely warning, those records are not protected by FERPA. 20 U.S.C. §1232g(a)(4)(B)(ii). ➢ However, timely warning reports must withhold the names and other identifying information about victims as confidential. 34 C.F.R. §668.46(e). <u>Emergency Response Procedures</u> ➢ The Clery Act requires institutions to have and disclose emergency response and procedures. As part of these procedures, institutions must immediately notify the campus community about *any* significant emergency or dangerous condition that may pose an immediate threat to the health or safety of students or employees occurring on the campus. 20 U.S.C. §485f(1)(J)(1)(i). ➢ An institution that follows its emergency notification procedures is not required to issue a timely warning based on the same circumstances; however, the institution must provide adequate follow-up information to the community as needed. 34 C.F.R. §668.46(e)(3). ➢ FERPA recognizes that information can, in the case of an emergency, be released without consent when needed to protect the health and safety of others. 34 C.F.R. §99.36(a).

UNITED STATES DEPARTMENT OF EDUCATION
OFFICE FOR CIVIL RIGHTS

THE ASSISTANT SECRETARY

Questions and Answers on Title IX and Sexual Violence[1]

Title IX of the Education Amendments of 1972 ("Title IX")[2] is a federal civil rights law that prohibits discrimination on the basis of sex in federally funded education programs and activities. All public and private elementary and secondary schools, school districts, colleges, and universities receiving any federal financial assistance (hereinafter "schools", "recipients", or "recipient institutions") must comply with Title IX.[3]

On April 4, 2011, the Office for Civil Rights (OCR) in the U.S. Department of Education issued a Dear Colleague Letter on student-on-student sexual harassment and sexual violence ("DCL").[4] The DCL explains a school's responsibility to respond promptly and effectively to sexual violence against students in accordance with the requirements of Title IX.[5] Specifically, the DCL:

- Provides guidance on the unique concerns that arise in sexual violence cases, such as a school's independent responsibility under Title IX to investigate (apart from any separate criminal investigation by local police) and address sexual violence.

---

[1] The Department has determined that this document is a "significant guidance document" under the Office of Management and Budget's Final Bulletin for Agency Good Guidance Practices, 72 Fed. Reg. 3432 (Jan. 25, 2007), *available at* www.whitehouse.gov/sites/default/files/omb/fedreg/2007/012507_good_guidance.pdf. The Office for Civil Rights (OCR) issues this and other policy guidance to provide recipients with information to assist them in meeting their obligations, and to provide members of the public with information about their rights, under the civil rights laws and implementing regulations that we enforce. OCR's legal authority is based on those laws and regulations. This guidance does not add requirements to applicable law, but provides information and examples to inform recipients about how OCR evaluates whether covered entities are complying with their legal obligations. If you are interested in commenting on this guidance, please send an e-mail with your comments to OCR@ed.gov, or write to the following address: Office for Civil Rights, U.S. Department of Education, 400 Maryland Avenue, SW, Washington, D.C. 20202.

[2] 20 U.S.C. § 1681 *et seq*.

[3] Throughout this document the term "schools" refers to recipients of federal financial assistance that operate educational programs or activities. For Title IX purposes, at the elementary and secondary school level, the recipient generally is the school district; and at the postsecondary level, the recipient is the individual institution of higher education. An educational institution that is controlled by a religious organization is exempt from Title IX to the extent that the law's requirements conflict with the organization's religious tenets. 20 U.S.C. § 1681(a)(3); 34 C.F.R. § 106.12(a). For application of this provision to a specific institution, please contact the appropriate OCR regional office.

[4] Available at http://www.ed.gov/ocr/letters/colleague-201104.html.

[5] Although this document and the DCL focus on sexual violence, the legal principles generally also apply to other forms of sexual harassment.

- Provides guidance and examples about key Title IX requirements and how they relate to sexual violence, such as the requirements to publish a policy against sex discrimination, designate a Title IX coordinator, and adopt and publish grievance procedures.

- Discusses proactive efforts schools can take to prevent sexual violence.

- Discusses the interplay between Title IX, the Family Educational Rights and Privacy Act ("FERPA"),[6] and the Jeanne Clery Disclosure of Campus Security and Campus Crime Statistics Act ("Clery Act")[7] as it relates to a complainant's right to know the outcome of his or her complaint, including relevant sanctions imposed on the perpetrator.

- Provides examples of remedies and enforcement strategies that schools and OCR may use to respond to sexual violence.

The DCL supplements OCR's *Revised Sexual Harassment Guidance: Harassment of Students by School Employees, Other Students, or Third Parties*, issued in 2001 (*2001 Guidance*).[8] The *2001 Guidance* discusses in detail the Title IX requirements related to sexual harassment of students by school employees, other students, or third parties. The DCL and the *2001 Guidance* remain in full force and we recommend reading these Questions and Answers in conjunction with these documents.

In responding to requests for technical assistance, OCR has determined that elementary and secondary schools and postsecondary institutions would benefit from additional guidance concerning their obligations under Title IX to address sexual violence as a form of sexual harassment. The following questions and answers further clarify the legal requirements and guidance articulated in the DCL and the *2001 Guidance* and include examples of proactive efforts schools can take to prevent sexual violence and remedies schools may use to end such conduct, prevent its recurrence, and address its effects. In order to gain a complete understanding of these legal requirements and recommendations, this document should be read in full.

Authorized by

/s/

Catherine E. Lhamon
Assistant Secretary for Civil Rights

April 29, 2014

---

[6] 20 U.S.C. §1232g; 34 C.F.R. Part 99.
[7] 20 U.S.C. §1092(f).
[8] Available at http://www.ed.gov/ocr/docs/shguide.html.

should also explain to the student (again, before the student reveals information that he or she may wish to keep confidential) that, although the RA must report the names of the alleged perpetrator (if known), the student who experienced the alleged sexual violence, other students involved in the alleged sexual violence, as well as relevant facts, including the date, time, and location to the Title IX coordinator or other appropriate school designee, the school will protect the student's confidentiality to the greatest extent possible. Prior to providing information about the incident to the Title IX coordinator or other appropriate school designee, the RA should consult with the student about how to protect his or her safety and the details of what will be shared with the Title IX coordinator. The RA should explain to the student that reporting this information to the Title IX coordinator or other appropriate school designee does not necessarily mean that a formal complaint or investigation under the school's Title IX grievance procedure must be initiated if the student requests confidentiality. As discussed in questions E-1 and E-2, if the student requests confidentiality, the Title IX coordinator or other appropriate school designee responsible for evaluating requests for confidentiality should make every effort to respect this request and should evaluate the request in the context of the school's responsibility to provide a safe and nondiscriminatory environment for all students.

Regardless of whether a reporting obligation exists, all RAs should inform students of their right to file a Title IX complaint with the school and report a crime to campus or local law enforcement. If a student discloses sexual violence to an RA who is a responsible employee, the school will be deemed to have notice of the sexual violence even if the student does not file a Title IX complaint. Additionally, all RAs should provide students with information regarding on-campus resources, including victim advocacy, housing assistance, academic support, counseling, disability services, health and mental health services, and legal assistance. RAs should also be familiar with local rape crisis centers or other off-campus resources and provide this information to students.

E. Confidentiality and a School's Obligation to Respond to Sexual Violence

E-1. How should a school respond to a student's request that his or her name not be disclosed to the alleged perpetrator or that no investigation or disciplinary action be pursued to address the alleged sexual violence?

Answer: Students, or parents of minor students, reporting incidents of sexual violence sometimes ask that the students' names not be disclosed to the alleged perpetrators or that no investigation or disciplinary action be pursued to address the alleged sexual violence. OCR strongly supports a student's interest in confidentiality in cases involving sexual violence. There are situations in which a school must override a student's request

for confidentiality in order to meet its Title IX obligations; however, these instances will be limited and the information should only be shared with individuals who are responsible for handling the school's response to incidents of sexual violence. Given the sensitive nature of reports of sexual violence, a school should ensure that the information is maintained in a secure manner. A school should be aware that disregarding requests for confidentiality can have a chilling effect and discourage other students from reporting sexual violence. In the case of minors, state mandatory reporting laws may require disclosure, but can generally be followed without disclosing information to school personnel who are not responsible for handling the school's response to incidents of sexual violence.[25]

Even if a student does not specifically ask for confidentiality, to the extent possible, a school should only disclose information regarding alleged incidents of sexual violence to individuals who are responsible for handling the school's response. To improve trust in the process for investigating sexual violence complaints, a school should notify students of the information that will be disclosed, to whom it will be disclosed, and why. Regardless of whether a student complainant requests confidentiality, a school must take steps to protect the complainant as necessary, including taking interim measures before the final outcome of an investigation. For additional information on interim measures see questions G-1 to G-3.

For Title IX purposes, if a student requests that his or her name not be revealed to the alleged perpetrator or asks that the school not investigate or seek action against the alleged perpetrator, the school should inform the student that honoring the request may limit its ability to respond fully to the incident, including pursuing disciplinary action against the alleged perpetrator. The school should also explain that Title IX includes protections against retaliation, and that school officials will not only take steps to prevent retaliation but also take strong responsive action if it occurs. This includes retaliatory actions taken by the school and school officials. When a school knows or reasonably should know of possible retaliation by other students or third parties, including threats, intimidation, coercion, or discrimination (including harassment), it must take immediate

[25] The school should be aware of the alleged student perpetrator's right under the Family Educational Rights and Privacy Act ("FERPA") torequest to inspect and review information about the allegations if the information directly relates to the alleged student perpetrator and the information is maintained by the school as an education record. In such a case, the school must either redact the complainant's name and all identifying information before allowing the alleged perpetrator to inspect and review the sections of the complaint that relate to him or her, or must inform the alleged perpetrator of the specific information in the complaint that are about the alleged perpetrator. *See* 34 C.F.R. § 99.12(a) The school should also make complainants aware of this right and explain how it might affect the school's ability to maintain complete confidentiality.

and appropriate steps to investigate or otherwise determine what occurred. Title IX requires the school to protect the complainant and ensure his or her safety as necessary. See question K-1 regarding retaliation.

If the student still requests that his or her name not be disclosed to the alleged perpetrator or that the school not investigate or seek action against the alleged perpetrator, the school will need to determine whether or not it can honor such a request while still providing a safe and nondiscriminatory environment for all students, including the student who reported the sexual violence. As discussed in question C-3, the Title IX coordinator is generally in the best position to evaluate confidentiality requests. Because schools vary widely in size and administrative structure, OCR recognizes that a school may reasonably determine that an employee other than the Title IX coordinator, such as a sexual assault response coordinator, dean, or other school official, is better suited to evaluate such requests. Addressing the needs of a student reporting sexual violence while determining an appropriate institutional response requires expertise and attention, and a school should ensure that it assigns these responsibilities to employees with the capability and training to fulfill them. For example, if a school has a sexual assault response coordinator, that person should be consulted in evaluating requests for confidentiality. The school should identify in its Title IX policies and procedures the employee or employees responsible for making such determinations.

If the school determines that it can respect the student's request not to disclose his or her identity to the alleged perpetrator, it should take all reasonable steps to respond to the complaint consistent with the request. Although a student's request to have his or her name withheld may limit the school's ability to respond fully to an individual allegation of sexual violence, other means may be available to address the sexual violence. There are steps a school can take to limit the effects of the alleged sexual violence and prevent its recurrence without initiating formal action against the alleged perpetrator or revealing the identity of the student complainant. Examples include providing increased monitoring, supervision, or security at locations or activities where the misconduct occurred; providing training and education materials for students and employees; changing and publicizing the school's policies on sexual violence; and conducting climate surveys regarding sexual violence. In instances affecting many students, an alleged perpetrator can be put on notice of allegations of harassing behavior and be counseled appropriately without revealing, even indirectly, the identity of the student complainant. A school must also take immediate action as necessary to protect the student while keeping the identity of the student confidential. These actions may include providing support services to the student and changing living arrangements or course schedules, assignments, or tests.

F-3. How should a school proceed when campus or local law enforcement agencies are conducting a criminal investigation while the school is conducting a parallel Title IX investigation?

Answer: A school should not wait for the conclusion of a criminal investigation or criminal proceeding to begin its own Title IX investigation. Although a school may need to delay temporarily the fact-finding portion of a Title IX investigation while the police are gathering evidence, it is important for a school to understand that during this brief delay in the Title IX investigation, it must take interim measures to protect the complainant in the educational setting. The school should also continue to update the parties on the status of the investigation and inform the parties when the school resumes its Title IX investigation. For additional information on interim measures see questions G-1 to G-3.

If a school delays the fact-finding portion of a Title IX investigation, the school must promptly resume and complete its fact-finding for the Title IX investigation once it learns that the police department has completed its evidence gathering stage of the criminal investigation. The school should not delay its investigation until the ultimate outcome of the criminal investigation or the filing of any charges. OCR recommends that a school work with its campus police, local law enforcement, and local prosecutor's office to learn when the evidence gathering stage of the criminal investigation is complete. A school may also want to enter into a memorandum of understanding (MOU) or other agreement with these agencies regarding the protocols and procedures for referring allegations of sexual violence, sharing information, and conducting contemporaneous investigations. Any MOU or other agreement must allow the school to meet its Title IX obligation to resolve complaints promptly and equitably, and must comply with the Family Educational Rights and Privacy Act ("FERPA") and other applicable privacy laws.

The DCL states that in one instance a prosecutor's office informed OCR that the police department's evidence gathering stage typically takes three to ten calendar days, although the delay in the school's investigation may be longer in certain instances. OCR understands that this example may not be representative and that the law enforcement agency's process often takes more than ten days. OCR recognizes that the length of time for evidence gathering by criminal investigators will vary depending on the specific circumstances of each case.

- Conducting, in conjunction with student leaders, a campus climate check to assess the effectiveness of efforts to ensure that the school is free from sexual violence, and using that information to inform future proactive steps that the school will take;

- Targeted training for a group of students if, for example, the sexual violence created a hostile environment in a residence hall, fraternity or sorority, or on an athletic team; and

- Developing a protocol for working with local law enforcement as discussed in question F-3.

When a school is unable to conduct a full investigation into a particular incident (*i.e*., when it received a general report of sexual violence without any personally identifying information), it should consider remedies for the broader student population in response.

H-2. If, after an investigation, a school finds the alleged perpetrator responsible and determines that, as part of the remedies for the complainant, it must separate the complainant and perpetrator, how should the school accomplish this if both students share the same major and there are limited course options?

Answer: If there are limited sections of required courses offered at a school and both the complainant and perpetrator are required to take those classes, the school may need to make alternate arrangements in a manner that minimizes the burden on the complainant. For example, the school may allow the complainant to take the regular sections of the courses while arranging for the perpetrator to take the same courses online or through independent study.

H-3. What information must be provided to the complainant in the notice of the outcome?

Answer: Title IX requires both parties to be notified, in writing, about the outcome of both the complaint and any appeal. OCR recommends that a school provide written notice of the outcome to the complainant and the alleged perpetrator concurrently.

For Title IX purposes, a school must inform the complainant as to whether or not it found that the alleged conduct occurred, any individual remedies offered or provided to the complainant or any sanctions imposed on the perpetrator that directly relate to the complainant, and other steps the school has taken to eliminate the hostile environment, if the school finds one to exist, and prevent recurrence. The perpetrator should not be notified of the individual remedies offered or provided to the complainant.

Sanctions that directly relate to the complainant (but that may also relate to eliminating the hostile environment and preventing recurrence) include, but are not limited to, requiring that the perpetrator stay away from the complainant until both parties graduate, prohibiting the perpetrator from attending school for a period of time, or transferring the perpetrator to another residence hall, other classes, or another school. Additional steps the school has taken to eliminate the hostile environment may include counseling and academic support services for the complainant and other affected students. Additional steps the school has taken to prevent recurrence may include sexual violence training for faculty and staff, revisions to the school's policies on sexual violence, and campus climate surveys. Further discussion of appropriate remedies is included in question H-1.

In addition to the Title IX requirements described above, the Clery Act requires, and FERPA permits, postsecondary institutions to inform the complainant of the institution's final determination and any disciplinary sanctions imposed on the perpetrator in sexual violence cases (as opposed to all harassment and misconduct covered by Title IX) not just those sanctions that directly relate to the complainant.[33]

I. Appeals

I-1. What are the requirements for an appeals process?

Answer: While Title IX does not require that a school provide an appeals process, OCR does recommend that the school do so where procedural error or previously unavailable relevant evidence could significantly impact the outcome of a case or where a sanction is substantially disproportionate to the findings. If a school chooses to provide for an appeal of the findings or remedy or both, it must do so equally for both parties. The specific design of the appeals process is up to the school, as long as the entire grievance process, including any appeals, provides prompt and equitable resolutions of sexual violence complaints, and the school takes steps to protect the complainant in the educational setting during the process. Any individual or body handling appeals should be trained in the dynamics of and trauma associated with sexual violence.

If a school chooses to offer an appeals process it has flexibility to determine the type of review it will apply to appeals, but the type of review the school applies must be the same regardless of which party files the appeal.

---

[33] 20 U.S.C. § 1092(f) and 20 U.S.C. § 1232g(b)(6)(A).

UNITED STATES DEPARTMENT OF EDUCATION

OFFICE FOR CIVIL RIGHTS

THE ASSISTANT SECRETARY

April 4, 2011

Dear Colleague:

Education has long been recognized as the great equalizer in America. The U.S. Department of Education and its Office for Civil Rights (OCR) believe that providing all students with an educational environment free from discrimination is extremely important. The sexual harassment of students, including sexual violence, interferes with students' right to receive an education free from discrimination and, in the case of sexual violence, is a crime.

Title IX of the Education Amendments of 1972 (Title IX), 20 U.S.C. §§ 1681 *et seq.*, and its implementing regulations, 34 C.F.R. Part 106, prohibit discrimination on the basis of sex in education programs or activities operated by recipients of Federal financial assistance. Sexual harassment of students, which includes acts of sexual violence, is a form of sex discrimination prohibited by Title IX. In order to assist recipients, which include school districts, colleges, and universities (hereinafter "schools" or "recipients") in meeting these obligations, this letter[1] explains that the requirements of Title IX pertaining to sexual harassment also cover sexual violence, and lays out the specific Title IX requirements applicable to sexual violence.[2] Sexual violence, as that term is used in this letter, refers to physical sexual acts perpetrated against a person's will or where a person is incapable of giving consent due to the victim's use of drugs or alcohol. An individual also may be unable to give consent due to an intellectual or other disability. A number of different acts fall into the category of sexual violence, including rape,

[1] The Department has determined that this Dear Colleague Letter is a "significant guidance document" under the Office of Management and Budget's Final Bulletin for Agency Good Guidance Practices, 72 Fed. Reg. 3432 (Jan. 25, 2007), *available at:* http://www.whitehouse.gov/sites/default/files/omb/assets/regulatory_matters_pdf/012507_good_guidance.pdf. OCR issues this and other policy guidance to provide recipients with information to assist them in meeting their obligations, and to provide members of the public with information about their rights, under the civil rights laws and implementing regulations that we enforce. OCR's legal authority is based on those laws and regulations. This letter does not add requirements to applicable law, but provides information and examples to inform recipients about how OCR evaluates whether covered entities are complying with their legal obligations. If you are interested in commenting on this guidance, please send an e-mail with your comments to OCR@ed.gov, or write to us at the following address: Office for Civil Rights, U.S. Department of Education, 400 Maryland Avenue, SW, Washington, DC 20202.

[2] Use of the term "sexual harassment" throughout this document includes sexual violence unless otherwise noted. Sexual harassment also may violate Title IV of the Civil Rights Act of 1964 (42 U.S.C. § 2000c), which prohibits public school districts and colleges from discriminating against students on the basis of sex, among other bases. The U.S. Department of Justice enforces Title IV.

investigation will vary depending upon the nature of the allegations, the age of the student or students involved (particularly in elementary and secondary schools), the size and administrative structure of the school, and other factors. Yet as discussed in more detail below, the school's inquiry must in all cases be prompt, thorough, and impartial. In cases involving potential criminal conduct, school personnel must determine, consistent with State and local law, whether appropriate law enforcement or other authorities should be notified.[13]

Schools also should inform and obtain consent from the complainant (or the complainant's parents if the complainant is under 18 and does not attend a postsecondary institution) before beginning an investigation. If the complainant requests confidentiality or asks that the complaint not be pursued, the school should take all reasonable steps to investigate and respond to the complaint consistent with the request for confidentiality or request not to pursue an investigation. If a complainant insists that his or her name or other identifiable information not be disclosed to the alleged perpetrator, the school should inform the complainant that its ability to respond may be limited.[14] The school also should tell the complainant that Title IX prohibits retaliation, and that school officials will not only take steps to prevent retaliation but also take strong responsive action if it occurs.

As discussed in the *2001 Guidance*, if the complainant continues to ask that his or her name or other identifiable information not be revealed, the school should evaluate that request in the context of its responsibility to provide a safe and nondiscriminatory environment for all students. Thus, the school may weigh the request for confidentiality against the following factors: the seriousness of the alleged harassment; the complainant's age; whether there have been other harassment complaints about the same individual; and the alleged harasser's rights to receive information about the allegations if the information is maintained by the school as an "education record" under the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g; 34 C.F.R. Part 99.[15] The school should inform the complainant if it cannot ensure confidentiality. Even if the school cannot take disciplinary action against the alleged harasser because the complainant insists on confidentiality, it should pursue other steps to limit the effects of the alleged harassment and prevent its recurrence. Examples of such steps are discussed later in this letter.

Compliance with Title IX, such as publishing a notice of nondiscrimination, designating an employee to coordinate Title IX compliance, and adopting and publishing grievance procedures, can serve as preventive measures against harassment. Combined with education and training programs, these measures can help ensure that all students and employees recognize the

[13] In states with mandatory reporting laws, schools may be required to report certain incidents to local law enforcement or child protection agencies.

[14] Schools should refer to the *2001 Guidance* for additional information on confidentiality and the alleged perpetrator's due process rights.

[15] For example, the alleged harasser may have a right under FERPA to inspect and review portions of the complaint that directly relate to him or her. In that case, the school must redact the complainant's name and other identifying information before allowing the alleged harasser to inspect and review the sections of the complaint that relate to him or her. In some cases, such as those where the school is required to report the incident to local law enforcement or other officials, the school may not be able to maintain the complainant's confidentiality.

Title VII prohibits discrimination on the basis of sex.[26] OCR also uses a preponderance of the evidence standard when it resolves complaints against recipients. For instance, OCR's Case Processing Manual requires that a noncompliance determination be supported by the preponderance of the evidence when resolving allegations of discrimination under all the statutes enforced by OCR, including Title IX.[27] OCR also uses a preponderance of the evidence standard in its fund termination administrative hearings.[28] Thus, in order for a school's grievance procedures to be consistent with Title IX standards, the school must use a preponderance of the evidence standard (*i.e.*, it is more likely than not that sexual harassment or violence occurred). The "clear and convincing" standard (*i.e.*, it is highly probable or reasonably certain that the sexual harassment or violence occurred), currently used by some schools, is a higher standard of proof. Grievance procedures that use this higher standard are inconsistent with the standard of proof established for violations of the civil rights laws, and are thus not equitable under Title IX. Therefore, preponderance of the evidence is the appropriate standard for investigating allegations of sexual harassment or violence.

Throughout a school's Title IX investigation, including at any hearing, the parties must have an equal opportunity to present relevant witnesses and other evidence. The complainant and the alleged perpetrator must be afforded similar and timely access to any information that will be used at the hearing.[29] For example, a school should not conduct a pre-hearing meeting during which only the alleged perpetrator is present and given an opportunity to present his or her side of the story, unless a similar meeting takes place with the complainant; a hearing officer or disciplinary board should not allow only the alleged perpetrator to present character witnesses at a hearing; and a school should not allow the alleged perpetrator to review the complainant's

---

[26] *See*, *e.g.*, *Desert Palace, Inc. v. Costa*, 539 U.S. 90, 99 (2003) (noting that under the "conventional rule of civil litigation," the preponderance of the evidence standard generally applies in cases under Title VII); *Price Waterhouse v. Hopkins*, 490 U.S. 228, 252-55 (1989) (approving preponderance standard in Title VII sex discrimination case) (plurality opinion); *id.* at 260 (White, J., concurring in the judgment); *id.* at 261 (O'Connor, J., concurring in the judgment). The *2001 Guidance* noted (on page vi) that "[w]hile *Gebser* and *Davis* made clear that Title VII agency principles do not apply in determining liability for money damages under Title IX, the *Davis* Court also indicated, through its specific references to Title VII caselaw, that Title VII remains relevant in determining what constitutes hostile environment sexual harassment under Title IX." *See also Jennings v. Univ. of N.C.*, 482 F.3d 686, 695 (4th Cir. 2007) ("We look to case law interpreting Title VII of the Civil Rights Act of 1964 for guidance in evaluating a claim brought under Title IX.").

[27] OCR's Case Processing Manual is available on the Department's Web site, at http://www2.ed.gov/about/offices/list/ocr/docs/ocrcpm.html.

[28] The Title IX regulations adopt the procedural provisions applicable to Title VI of the Civil Rights Act of 1964. *See* 34 C.F.R. § 106.71 ("The procedural provisions applicable to Title VI of the Civil Rights Act of 1964 are hereby adopted and incorporated herein by reference."). The Title VI regulations apply the Administrative Procedure Act to administrative hearings required prior to termination of Federal financial assistance and require that termination decisions be "supported by and in accordance with the reliable, probative and substantial evidence." 5 U.S.C. § 556(d). The Supreme Court has interpreted "reliable, probative and substantial evidence" as a direction to use the preponderance standard. *See Steadman v. SEC*, 450 U.S. 91, 98-102 (1981).

[29] Access to this information must be provided consistent with FERPA. For example, if a school introduces an alleged perpetrator's prior disciplinary records to support a tougher disciplinary penalty, the complainant would not be allowed access to those records. Additionally, access should not be given to privileged or confidential information. For example, the alleged perpetrator should not be given access to communications between the complainant and a counselor or information regarding the complainant's sexual history.

occurred in a classroom during school hours with a single complainant.

(D) *Notice of Outcome*

Both parties must be notified, in writing, about the outcome of both the complaint and any appeal,[31] *i.e.*, whether harassment was found to have occurred. OCR recommends that schools provide the written determination of the final outcome to the complainant and the alleged perpetrator concurrently. Title IX does not require the school to notify the alleged perpetrator of the outcome before it notifies the complainant.

Due to the intersection of Title IX and FERPA requirements, OCR recognizes that there may be confusion regarding what information a school may disclose to the complainant.[32] FERPA generally prohibits the nonconsensual disclosure of personally identifiable information from a student's "education record." However, as stated in the *2001 Guidance*, FERPA permits a school to disclose to the harassed student information about the sanction imposed upon a student who was found to have engaged in harassment when the sanction directly relates to the harassed student. This includes an order that the harasser stay away from the harassed student, or that the harasser is prohibited from attending school for a period of time, or transferred to other classes or another residence hall.[33] Disclosure of other information in the student's "education record," including information about sanctions that do not relate to the harassed student, may result in a violation of FERPA.

Further, when the conduct involves a crime of violence or a non-forcible sex offense,[34] FERPA permits a postsecondary institution to disclose to the alleged victim the final results of a

[31] As noted previously, "outcome" does not refer to information about disciplinary sanctions unless otherwise noted.

[32] In 1994, Congress amended the General Education Provisions Act (GEPA), of which FERPA is a part, to state that nothing in GEPA "shall be construed to affect the applicability of title VI of the Civil Rights Act of 1964, title IX of Education Amendments of 1972, title V of the Rehabilitation Act of 1973, the Age Discrimination Act, or other statutes prohibiting discrimination, to any applicable program." 20 U.S.C. § 1221(d). The Department interprets this provision to mean that FERPA continues to apply in the context of Title IX enforcement, but if there is a direct conflict between the requirements of FERPA and the requirements of Title IX, such that enforcement of FERPA would interfere with the primary purpose of Title IX to eliminate sex-based discrimination in schools, the requirements of Title IX override any conflicting FERPA provisions. *See 2001 Guidance* at vii.

[33] This information directly relates to the complainant and is particularly important in sexual harassment cases because it affects whether a hostile environment has been eliminated. Because seeing the perpetrator may be traumatic, a complainant in a sexual harassment case may continue to be subject to a hostile environment if he or she does not know when the perpetrator will return to school or whether he or she will continue to share classes or a residence hall with the perpetrator. This information also directly affects a complainant's decision regarding how to work with the school to eliminate the hostile environment and prevent its recurrence. For instance, if a complainant knows that the perpetrator will not be at school or will be transferred to other classes or another residence hall for the rest of the year, the complainant may be less likely to want to transfer to another school or change classes, but if the perpetrator will be returning to school after a few days or weeks, or remaining in the complainant's classes or residence hall, the complainant may want to transfer schools or change classes to avoid contact. Thus, the complainant cannot make an informed decision about how best to respond without this information.

[34] Under the FERPA regulations, crimes of violence include arson; assault offenses (aggravated assault, simple assault, intimidation); burglary; criminal homicide (manslaughter by negligence); criminal homicide (murder and

disciplinary proceeding against the alleged perpetrator, regardless of whether the institution concluded that a violation was committed.[35] Additionally, a postsecondary institution may disclose to anyone—not just the alleged victim—the final results of a disciplinary proceeding if it determines that the student is an alleged perpetrator of a crime of violence or a non-forcible sex offense, and, with respect to the allegation made, the student has committed a violation of the institution's rules or policies.[36]

Postsecondary institutions also are subject to additional rules under the Clery Act. This law, which applies to postsecondary institutions that participate in Federal student financial aid programs, requires that "both the accuser and the accused must be informed of the outcome[37] of any institutional disciplinary proceeding brought alleging a sex offense."[38] Compliance with this requirement does not constitute a violation of FERPA. Furthermore, the FERPA limitations on redisclosure of information do not apply to information that postsecondary institutions are required to disclose under the Clery Act.[39] Accordingly, postsecondary institutions may not require a complainant to abide by a nondisclosure agreement, in writing or otherwise, that would prevent the redisclosure of this information.

Steps to Prevent Sexual Harassment and Sexual Violence and Correct its Discriminatory Effects on the Complainant and Others

Education and Prevention

In addition to ensuring full compliance with Title IX, schools should take proactive measures to prevent sexual harassment and violence. OCR recommends that all schools implement preventive education programs and make victim resources, including comprehensive victim services, available. Schools may want to include these education programs in their (1) orientation programs for new students, faculty, staff, and employees; (2) training for students who serve as advisors in residence halls; (3) training for student athletes and coaches; and (4) school assemblies and "back to school nights." These programs should include a

---

non-negligent manslaughter); destruction, damage or vandalism of property; kidnapping/abduction; robbery; and forcible sex offenses. Forcible sex offenses are defined as any sexual act directed against another person forcibly or against that person's will, or not forcibly or against the person's will where the victim is incapable of giving consent. Forcible sex offenses include rape, sodomy, sexual assault with an object, and forcible fondling. Non-forcible sex offenses are incest and statutory rape. 34 C.F.R. Part 99, App. A.

[35] 34 C.F.R. § 99.31(a)(13). For purposes of 34 C.F.R. §§ 99.31(a)(13)-(14), disclosure of "final results" is limited to the name of the alleged perpetrator, any violation found to have been committed, and any sanction imposed against the perpetrator by the school. 34 C.F.R. § 99.39.

[36] 34 C.F.R. § 99.31(a)(14).

[37] For purposes of the Clery Act, "outcome" means the institution's final determination with respect to the alleged sex offense and any sanctions imposed against the accused. 34 C.F.R. § 668.46(b)(11)(vi)(B).

[38] 34 C.F.R. § 668.46(b)(11)(vi)(B). Under the Clery Act, forcible sex offenses are defined as any sexual act directed against another person forcibly or against that person's will, or not forcibly or against the person's will where the person is incapable of giving consent. Forcible sex offenses include forcible rape, forcible sodomy, sexual assault with an object, and forcible fondling. Non-forcible sex offenses include incest and statutory rape. 34 C.F.R. Part 668, Subpt. D, App. A.

[39] 34 C.F.R. § 99.33(c).

- arranging for the complainant to re-take a course or withdraw from a class without penalty, including ensuring that any changes do not adversely affect the complainant's academic record; and
- reviewing any disciplinary actions taken against the complainant to see if there is a causal connection between the harassment and the misconduct that may have resulted in the complainant being disciplined.[43]

Remedies for the broader student population might include, but are not limited to:

Counseling and Training

- offering counseling, health, mental health, or other holistic and comprehensive victim services to all students affected by sexual harassment or sexual violence, and notifying students of campus and community counseling, health, mental health, and other student services;
- designating an individual from the school's counseling center to be "on call" to assist victims of sexual harassment or violence whenever needed;
- training the Title IX coordinator and any other employees who are involved in processing, investigating, or resolving complaints of sexual harassment or sexual violence, including providing training on:
    - the school's Title IX responsibilities to address allegations of sexual harassment or violence
    - how to conduct Title IX investigations
    - information on the link between alcohol and drug abuse and sexual harassment or violence and best practices to address that link;
- training all school law enforcement unit personnel on the school's Title IX responsibilities and handling of sexual harassment or violence complaints;
- training all employees who interact with students regularly on recognizing and appropriately addressing allegations of sexual harassment or violence under Title IX; and
- informing students of their options to notify proper law enforcement authorities, including school and local police, and the option to be assisted by school employees in notifying those authorities.

Development of Materials and Implementation of Policies and Procedures

- developing materials on sexual harassment and violence, which should be distributed to students during orientation and upon receipt of complaints, as well as widely posted throughout school buildings and residence halls, and which should include:
    - what constitutes sexual harassment or violence
    - what to do if a student has been the victim of sexual harassment or violence
    - contact information for counseling and victim services on and off school grounds
    - how to file a complaint with the school
    - how to contact the school's Title IX coordinator

[43] For example, if the complainant was disciplined for skipping a class in which the harasser was enrolled, the school should review the incident to determine if the complainant skipped the class to avoid contact with the harasser.

    - what the school will do to respond to allegations of sexual harassment or violence, including the interim measures that can be taken
- requiring the Title IX coordinator to communicate regularly with the school's law enforcement unit investigating cases and to provide information to law enforcement unit personnel regarding Title IX requirements;[44]
- requiring the Title IX coordinator to review all evidence in a sexual harassment or sexual violence case brought before the school's disciplinary committee to determine whether the complainant is entitled to a remedy under Title IX that was not available through the disciplinary committee;[45]
- requiring the school to create a committee of students and school officials to identify strategies for ensuring that students:
    - know the school's prohibition against sex discrimination, including sexual harassment and violence
    - recognize sex discrimination, sexual harassment, and sexual violence when they occur
    - understand how and to whom to report any incidents
    - know the connection between alcohol and drug abuse and sexual harassment or violence
    - feel comfortable that school officials will respond promptly and equitably to reports of sexual harassment or violence;
- issuing new policy statements or other steps that clearly communicate that the school does not tolerate sexual harassment and violence and will respond to any incidents and to any student who reports such incidents; and
- revising grievance procedures used to handle sexual harassment and violence complaints to ensure that they are prompt and equitable, as required by Title IX.

School Investigations and Reports to OCR

- conducting periodic assessments of student activities to ensure that the practices and behavior of students do not violate the school's policies against sexual harassment and violence;
- investigating whether any other students also may have been subjected to sexual harassment or violence;
- investigating whether school employees with knowledge of allegations of sexual harassment or violence failed to carry out their duties in responding to those allegations;
- conducting, in conjunction with student leaders, a school or campus "climate check" to assess the effectiveness of efforts to ensure that the school is free from sexual harassment and violence, and using the resulting information to inform future proactive steps that will be taken by the school; and

[44] Any personally identifiable information from a student's education record that the Title IX coordinator provides to the school's law enforcement unit is subject to FERPA's nondisclosure requirements.

[45] For example, the disciplinary committee may lack the power to implement changes to the complainant's class schedule or living situation so that he or she does not come in contact with the alleged perpetrator.

REVISED SEXUAL HARASSMENT GUIDANCE: HARASSMENT OF STUDENTS BY SCHOOL EMPLOYEES, OTHER STUDENTS, OR THIRD PARTIES

TITLE IX

January 2001

U.S. Department of Education
Office for Civil Rights

the words used to define hostile environment harassment in the 1997 guidance (see, e.g., 62 FR 12041, "conduct of a sexual nature is sufficiently severe, persistent, or pervasive to limit a student's ability to participate in or benefit from the education program, or to create a hostile or abusive educational environment"), the definitions are consistent. Both the Court's and the Department's definitions are contextual descriptions intended to capture the same concept -– that under Title IX, the conduct must be sufficiently serious that it adversely affects a student's ability to participate in or benefit from the school's program. In determining whether harassment is actionable, both Davis and the Department tell schools to look at the "constellation of surrounding circumstances, expectations, and relationships" (526 U.S. at 651 (citing Oncale)), and the Davis Court cited approvingly to the underlying core factors described in the 1997 guidance for evaluating the context of the harassment. Second, schools benefit from consistency and simplicity in understanding what is sexual harassment for which the school must take responsive action. A multiplicity of definitions would not serve this purpose.

Several commenters suggested that we develop a unique Title IX definition of harassment that does not rely on Title VII and that takes into account the special relationship of schools to students. Other commenters, by contrast, commended OCR for recognizing that Gebser and Davis did not alter the definition of hostile environment sexual harassment found in OCR's 1997 guidance, which derives from Title VII caselaw, and asked us to strengthen the point. While Gebser and Davis made clear that Title VII agency principles do not apply in determining liability for money damages under Title IX, the Davis Court also indicated, through its specific references to Title VII caselaw, that Title VII remains relevant in determining what constitutes hostile environment sexual harassment under Title IX. We also believe that the factors described in both the 1997 guidance and the revised guidance to determine whether sexual harassment has occurred provide the necessary flexibility for taking into consideration the age and maturity of the students involved and the nature of the school environment.

Effective Response

One commenter suggested that the change in the guidance from "appropriate response" to "effective response" implies a change in OCR policy that requires omniscience of schools. We disagree. Effectiveness has always been the measure of an adequate response under Title IX. This does not mean a school must overreact out of fear of being judged inadequate. Effectiveness is measured based on a reasonableness standard. Schools do not have to know beforehand that their response will be effective. However, if their initial steps are ineffective in stopping the harassment, reasonableness may require a series of escalating steps.

The Relationship Between FERPA and Title IX

In the development of both the 1997 guidance and the current revisions to the guidance, commenters raised concerns about the interrelation of the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, and Title IX. The concerns relate to two issues: (1) the harassed student's right to information about the outcome of a sexual harassment complaint against another student, including information about sanctions imposed on a student found guilty of harassment; and (2) the due process rights of

individuals, including teachers, accused of sexual harassment by a student, to obtain information about the identity of the complainant and the nature of the allegations.

FERPA generally forbids disclosure of information from a student's "education record" without the consent of the student (or the student's parent). Thus, FERPA may be relevant when the person found to have engaged in harassment is another student, because written information about the complaint, investigation, and outcome is part of the harassing student's education record. Title IX is also relevant because it is an important part of taking effective responsive action for the school to inform the harassed student of the results of its investigation and whether it counseled, disciplined, or otherwise sanctioned the harasser. This information can assure the harassed student that the school has taken the student's complaint seriously and has taken steps to eliminate the hostile environment and prevent the harassment from recurring.

The Department currently interprets FERPA as not conflicting with the Title IX requirement that the school notify the harassed student of the outcome of its investigation, i.e., whether or not harassment was found to have occurred, because this information directly relates to the victim. It has been the Department's position that there is a potential conflict between FERPA and Title IX regarding disclosure of sanctions, and that FERPA generally prevents a school from disclosing to a student who complained of harassment information about the sanction or discipline imposed upon a student who was found to have engaged in that harassment.[3]

There is, however, an additional statutory provision that may apply to this situation. In 1994, as part of the Improving America's Schools Act, Congress amended the General Education Provisions Act (GEPA) -– of which FERPA is a part -– to state that nothing in GEPA "shall be construed to affect the applicability of … title IX of the Education Amendments of 1972…."[4] The Department interprets this provision to mean that FERPA continues to apply in the context of Title IX enforcement, but if there is a direct conflict between requirements of FERPA and requirements of Title IX, such that enforcement of FERPA would interfere with the primary purpose of Title IX to eliminate sex-based discrimination in schools, the requirements of Title IX override any conflicting FERPA provisions. The Department is in the process of developing a consistent approach and specific factors for implementing this provision. OCR and the Department's Family Policy Compliance Office (FPCO) intend to issue joint guidance, discussing specific areas of potential conflict between FERPA and Title IX.

---

[3] Exceptions include the case of a sanction that directly relates to the person who was harassed (e.g., an order that the harasser stay away from the harassed student), or sanctions related to offenses for which there is a statutory exception, such as crimes of violence or certain sex offenses in postsecondary institutions.

[4] 20 U.S.C. 1221(d). A similar amendment was originally passed in 1974 but applied only to Title VI of the Civil Rights Act of 1964 (prohibiting race discrimination by recipients). The 1994 amendments also extended 20 U.S.C. 1221(d) to Section 504 of the Rehabilitation Act of 1973 (prohibiting disability-based discrimination by recipients) and to the Age Discrimination Act.

FERPA is also relevant when a student accuses a teacher or other employee of sexual harassment, because written information about the allegations is contained in the student's education record. The potential conflict arises because, while FERPA protects the privacy of the student accuser, the accused individual may need the name of the accuser and information regarding the nature of the allegations in order to defend against the charges. The 1997 guidance made clear that neither FERPA nor Title IX override any federally protected due process rights of a school employee accused of sexual harassment.

Several commenters urged the Department to expand and strengthen this discussion. They argue that in many instances a school's failure to provide information about the name of the student accuser and the nature of the allegations seriously undermines the fairness of the investigative and adjudicative process. They also urge the Department to include a discussion of the need for confidentiality as to the identity of the individual accused of harassment because of the significant harm that can be caused by false accusations. We have made several changes to the guidance, including an additional discussion regarding the confidentiality of a person accused of harassment and a new heading entitled "Due Process Rights of the Accused," to address these concerns.

with a different instructor; provide tutoring; make tuition adjustments; offer reimbursement for professional counseling; or take other measures that are appropriate to the circumstances. As another example, if a school delays responding or responds inappropriately to information about harassment, such as a case in which the school ignores complaints by a student that he or she is being sexually harassed by a classmate, the school will be required to remedy the effects of the harassment that could have been prevented had the school responded promptly and effectively.

Finally, a school should take steps to prevent any further harassment[94] and to prevent any retaliation against the student who made the complaint (or was the subject of the harassment), against the person who filed a complaint on behalf of a student, or against those who provided information as witnesses.[95] At a minimum, this includes making sure that the harassed students and their parents know how to report any subsequent problems and making follow-up inquiries to see if there have been any new incidents or any retaliation. To prevent recurrences, counseling for the harasser may be appropriate to ensure that he or she understands what constitutes harassment and the effects it can have. In addition, depending on how widespread the harassment was and whether there have been any prior incidents, the school may need to provide training for the larger school community to ensure that students, parents, and teachers can recognize harassment if it recurs and know how to respond.[96]

B. Confidentiality

The scope of a reasonable response also may depend upon whether a student, or parent of a minor student, reporting harassment asks that the student's name not be disclosed to the harasser or that nothing be done about the alleged harassment. In all cases, a school should discuss confidentiality standards and concerns with the complainant initially. The school should inform the student that a confidentiality request may limit the school's ability to respond. The school also should tell the student that Title IX prohibits retaliation and that, if he or she is afraid of reprisals from the alleged harasser, the school will take steps to prevent retaliation and will take strong responsive actions if retaliation occurs. If the student continues to ask that his or her name not be revealed, the school should take all reasonable steps to investigate and respond to the complaint consistent with the student's request as long as doing so does not prevent the school from responding effectively to the harassment and preventing harassment of other students.

OCR enforces Title IX consistent with the federally protected due process rights of public school students and employees. Thus, for example, if a student, who was the only student harassed, insists that his or her name not be revealed, and the alleged harasser could not respond to the charges of sexual harassment without that information, in evaluating the school's response, OCR would not expect disciplinary action against an alleged harasser.

At the same time, a school should evaluate the confidentiality request in the context of its responsibility to provide a safe and nondiscriminatory environment for all students. The factors that a school may consider in this regard include the seriousness of the alleged harassment, the age of the student harassed, whether there have been other complaints or reports of harassment against the alleged harasser, and the rights of the

accused individual to receive information about the accuser and the allegations if a formal proceeding with sanctions may result.[97]

Similarly, a school should be aware of the confidentiality concerns of an accused employee or student. Publicized accusations of sexual harassment, if ultimately found to be false, may nevertheless irreparably damage the reputation of the accused. The accused individual's need for confidentiality must, of course, also be evaluated based on the factors discussed in the preceding paragraph in the context of the school's responsibility to ensure a safe environment for students.

Although a student's request to have his or her name withheld may limit the school's ability to respond fully to an individual complaint of harassment, other means may be available to address the harassment. There are steps a recipient can take to limit the effects of the alleged harassment and prevent its recurrence without initiating formal action against the alleged harasser or revealing the identity of the complainant. Examples include conducting sexual harassment training for the school site or academic department where the problem occurred, taking a student survey concerning any problems with harassment, or implementing other systemic measures at the site or department where the alleged harassment has occurred.

In addition, by investigating the complaint to the extent possible — including by reporting it to the Title IX coordinator or other responsible school employee designated pursuant to Title IX — the school may learn about or be able to confirm a pattern of harassment based on claims by different students that they were harassed by the same individual. In some situations there may be prior reports by former students who now might be willing to come forward and be identified, thus providing a basis for further corrective action. In instances affecting a number of students (for example, a report from a student that an instructor has repeatedly made sexually explicit remarks about his or her personal life in front of an entire class), an individual can be put on notice of allegations of harassing behavior and counseled appropriately without revealing, even indirectly, the identity of the student who notified the school. Those steps can be very effective in preventing further harassment.

C. Response to Other Types of Notice

The previous two sections deal with situations in which a student or parent of a student who was harassed reports or complains of harassment or in which a responsible school employee directly observes sexual harassment of a student. If a school learns of harassment through other means, for example, if information about harassment is received from a third party (such as from a witness to an incident or an anonymous letter or telephone call), different factors will affect the school's response. These factors include the source and nature of the information; the seriousness of the alleged incident; the specificity of the information; the objectivity and credibility of the source of the report; whether any individuals can be identified who were subjected to the alleged harassment; and whether those individuals want to pursue the matter. If, based on these factors, it is reasonable for the school to investigate and it can confirm the allegations, the considerations described in the previous sections concerning interim measures and appropriate responsive action will apply.

prohibited sex discrimination, a school's general policy and procedures relating to sex discrimination complaints will not be considered effective.[101]

OCR has identified a number of elements in evaluating whether a school's grievance procedures are prompt and equitable, including whether the procedures provide for —

- Notice to students, parents of elementary and secondary students, and employees of the procedure, including where complaints may be filed;
- Application of the procedure to comp laints alleging harassment carried out by employees, other students, or third parties;
- Adequate, reliable, and impartial investigation of complaints, including the opportunity to present witnesses and other evidence;
- Designated and reasonably prompt timeframes for the major stages of the complaint process;
- Notice to the parties of the outcome of the complaint;[102] and
- An assurance that the school will take steps to prevent recurrence of any harassment and to correct its discriminatory effects on the complainant and others, if appropriate.[103]

Many schools also provide an opportunity to appeal the findings or remedy, or both. In addition, because retaliation is prohibited by Title IX, schools may want to include a provision in their procedures prohibiting retaliation against any individual who files a complaint or participates in a harassment inquiry.

Procedures adopted by schools will vary considerably in detail, specificity, and components, reflecting differences in audiences, school sizes and administrative structures, State or local legal requirements, and past experience. In addition, whether complaint resolutions are timely will vary depending on the complexity of the investigation and the severity and extent of the harassment. During the investigation it is a good practice for schools to inform students who have alleged harassment about the status of the investigation on a periodic basis.

A grievance procedure applicable to sexual harassment complaints cannot be prompt or equitable unless students know it exists, how it works, and how to file a complaint. Thus, the procedures should be written in language appropriate to the age of the school's students, easily understood, and widely disseminated. Distributing the procedures to administrators, or including them in the school's administrative or policy manual, may not by itself be an effective way of providing notice, as these publications are usually not widely circulated to and understood by all members of the school community. Many schools ensure adequate notice to students by having copies of the procedures available at various locations throughout the school or campus; publishing the procedures as a separate document; including a summary of the procedures in major publications issued by the school, such as handbooks and catalogs for students, parents of elementary and secondary students, faculty, and staff; and identifying individuals who can explain how the procedures work.

X. Due Process Rights of the Accused

A public school's employees have certain due process rights under the United States Constitution. The Constitution also guarantees due process to students in public and State-supported schools who are accused of certain types of infractions. The rights established under Title IX must be interpreted consistent with any federally guaranteed due process rights involved in a complaint proceeding. Furthermore, the Family Educational Rights and Privacy Act (FERPA) does not override federally protected due process rights of persons accused of sexual harassment. Procedures that ensure the Title IX rights of the complainant, while at the same time according due process to both parties involved, will lead to sound and supportable decisions. Of course, schools should ensure that steps to accord due process rights do not restrict or unnecessarily delay the protections provided by Title IX to the complainant. In both public and private schools, additional or separate rights may be created for employees or students by State law, institutional regulations and policies, such as faculty or student handbooks, and collective bargaining agreements. Schools should be aware of these rights and their legal responsibilities to individuals accused of harassment.

XI. First Amendment

In cases of alleged harassment, the protections of the First Amendment must be considered if issues of speech or expression are involved.[112] Free speech rights apply in the classroom (e.g., classroom lectures and discussions)[113] and in all other education programs and activities of public schools (e.g., public meetings and speakers on campus; campus debates, school plays and other cultural events[114]; and student newspapers, journals, and other publications[115]). In addition, First Amendment rights apply to the speech of students and teachers.[116]

Title IX is intended to protect students from sex discrimination, not to regulate the content of speech. OCR recognizes that the offensiveness of a particular expression as perceived by some students, standing alone, is not a legally sufficient basis to establish a sexually hostile environment under Title IX.[117] In order to establish a violation of Title IX, the harassment must be sufficiently serious to deny or limit a student's ability to participate in or benefit from the education program.[118]

Moreover, in regulating the conduct of its students and its faculty to prevent or redress discrimination prohibited by Title IX (e.g., in responding to harassment that is sufficiently serious as to create a hostile environment), a school must formulate, interpret, and apply its rules so as to protect academic freedom and free speech rights. For instance, while the First Amendment may prohibit a school from restricting the right of students to express opinions about one sex that may be considered derogatory, the school can take steps to denounce those opinions and ensure that competing views are heard. The age of the students involved and the location or forum may affect how the school can respond consistently with the First Amendment.[119] As an example of the application of free speech rights to allegations of sexual harassment, consider the following:

Example 1: In a college level creative writing class, a professor's required reading list includes excerpts from literary classics that contain descriptions of explicit

necessary in situations in which counseling, separating the parties, and warnings of possible discipline were ineffective in ending the harassing behavior).

[91] Offering assistance in changing living arrangements is one of the actions required of colleges and universities by the Campus Security Act in cases of rape and sexual assault. See 20 U.S.C. 1092(f).

[92] See section on "Harassment by Other Students or Third Parties."

[93] University of California at Santa Cruz, OCR Case No. 09-93-2141 (extensive individual and group counseling); Eden Prairie Schools, Dist. #272, OCR Case No. 05-92-1174 (counseling).

[94] Even if the harassment stops without the school's involvement, the school may still need to take steps to prevent or deter any future harassment –– to inform the school community that harassment will not be tolerated. Wills v. Brown University, 184 F.3d 20, 28 (1st Cir. 1999) (difficult problems are posed in balancing a student's request for anonymity or limited disclosure against the need to prevent future harassment); Fuller v. City of Oakland, 47 F.3d 1522, 1528-29 (9th Cir. 1995) (Title VII case).

[95] 34 CFR 106.8(b) and 106.71, incorporating by reference 34 CFR 100.7(e). The Title IX regulations prohibit intimidation, threats, coercion, or discrimination against any individual for the purpose of interfering with any right or privilege secured by Title IX.

[96] Tacoma School Dist. No. 10, OCR Case No. 10-94-1079 (due to the large number of students harassed by an employee, the extended period of time over which the harassment occurred, and the failure of several of the students to report the harassment, the school committed as part of corrective action plan to providing training for students); Los Medanos College, OCR Case No. 09-84-2092 (as part of corrective action plan, school committed to providing sexual harassment seminar for campus employees); Sacramento City Unified School Dist., OCR Case No. 09-83-1063 (same as to workshops for management and administrative personnel and in-service training for non-management personnel).

[97] In addition, if information about the incident is contained in an "education record" of the student alleging the harassment, as defined in the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. 1232g, the school should consider whether FERPA would prohibit the school from disclosing information without the student's consent. Id. In evaluating whether FERPA would limit disclosure, the Department does not interpret FERPA to override any federally protected due process rights of a school employee accused of harassment.

[98] 34 CFR 106.8(b). This requirement has been part of the Title IX regulations since their inception in 1975. Thus, schools have been required to have these procedures in place since that time. At the elementary and secondary level, this responsibility generally lies

with the school district. At the postsecondary level, there may be a procedure for a particular campus or college or for an entire university system.

[99] Fenton Community High School Dist. #100, OCR Case 05-92-1104.

[100] While a school is required to have a grievance procedure under which complaints of sex discrimination (including sexual harassment) can be filed, the same procedure may also be used to address other forms of discrimination.

[101] See generally Meritor, 477 U.S. at 72-73 (holding that "mere existence of a grievance procedure" for discrimination does not shield an employer from a sexual harassment claim).

[102] The Family Educational Rights and Privacy Act (FERPA) does not prohibit a student from learning the outcome of her complaint, i.e., whether the complaint was found to be credible and whether harassment was found to have occurred. It is the Department's current position under FERPA that a school cannot release information to a complainant regarding disciplinary action imposed on a student found guilty of harassment if that information is contained in a student's education record unless — (1) the information directly relates to the complainant (e.g., an order requiring the student harasser not to have contact with the complainant); or (2) the harassment involves a crime of violence or a sex offense in a postsecondary institution. See note 97. If the alleged harasser is a teacher, administrator, or other non-student employee, FERPA would not limit the school's ability to inform the complainant of any disciplinary action taken.

[103] The section in the guidance on "Recipient's Response" provides examples of reasonable and appropriate corrective action.

[104] 34 CFR 106.8(a).

[105] Id.

[106] See Meritor, 477 U.S. at 72-73.

[107] University of California, Santa Cruz, OCR Case No. 09-93-2131. This is true for formal as well as informal complaints. See University of Maine at Machias, OCR Case No. 01-94-6001 (school's new procedures not found in violation of Title IX in part because they require written records for informal as well as formal resolutions). These records need not be kept in a student's or employee's individual file, but instead may be kept in a central confidential location.

[108] For example, in Cape Cod Community College, OCR Case No. 01-93-2047, the College was found to have violated Title IX in part because the person identified by the school as the Title IX coordinator was unfamiliar with Title IX, had no training, and did not even realize he was the coordinator.

NACUANOTES
June 19, 2009
Volume 7 No. 8

TOPIC:

FERPA AND CAMPUS SAFETY
(UPDATE to Vol 5 No.4, August 6, 2007 issue)

INTRODUCTION:

Campus safety is a top priority for colleges and universities. Sometimes a student's statements or behaviors raise concerns about the safety of the student or others. To prevent harm from occurring, college administrators, faculty, and staff who are aware of such statements or behaviors may want to tell someone else – another campus employee, a parent, an outside health care professional, or a law enforcement officer about their concern. But they do not know exactly who to tell. And they often fear that the Family Educational Rights and Privacy Act ("FERPA") [1], the federal statute that governs disclosure of student records and information, limits those with whom they may share information found in the student's records. Therefore, they unnecessarily and unwisely conclude that the safest course is simply telling no one or saying nothing.

Misunderstandings about FERPA generate a lot of concern about the propriety of communicating critical information in an emergency. The information in this NACUANOTE demonstrates that FERPA is not an obstacle to appropriate and desirable cautionary communications intended to protect student, campus, or public safety. While emergency situations are not governed solely by FERPA, and other state or federal laws beyond the scope of this NACUANOTE may impose additional legal restrictions, preventing harm to individuals should take precedence.

DISCUSSION:

Question: What does FERPA restrict?

Answer: FERPA limits the disclosure of information from student "education records," a term that the law defines quite broadly and that is *not* limited to "academic" records.

"Education records" include virtually all records maintained by an educational institution, in any format, that are "directly related" to one or more of its past or present students [2]. A record is "directly related" to a student if it is "personally identifiable" to the student [3]. A record is "personally identifiable" to a student if it expressly identifies the student on its face by name, address, ID number, or other such common identifier. A record is also personally identifiable if it 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" – in other words, if it contains enough demographic or other information that it points to a single student [4]. For example, a disciplinary record about an unnamed male student likely would not, without more, be personally identifiable, but a disciplinary record about an unnamed male sophomore political science major who lives in Smith Hall, plays on the soccer team, and is a resident of Wyoming likely would "name" the particular student. A record may also be "personally identifiable" because of commonly known information external to the record. For example, a request to provide information about all university sanctions imposed for cheating in the past five years might include a large enough number of instances not to identify any of the students. On the other hand, a request to provide information about sanctions imposed against student athletes for cheating in the past two weeks, at a time when a well-known student athlete suddenly is not playing or practicing with the team, would be a request seeking personally identifiable information in that context because it could be used to confirm or deny rumors regarding the reason for the student's absence.

Despite the name "education records," there is no requirement that a record be "educational" or "academic" in nature to qualify. Moreover, the defintition of "education records" does not give institutions any discretion to determine for themselves what is or isn't an "education record" or to "treat" certain records as non-education records, even though they meet the statutory definition. Thus, "education records" include not only registrar's office records, transcripts, papers, exams and the like, but also non-academic student information database systems [5], class schedules [6], financial aid records [7], financial account records [8], disability accommodation records [9], disciplinary records [10], and even "unofficial" files, photographs, e-mail messages [11], hand-scrawled Post-it notes, and records that are publicly available elsewhere [12] or that the student herself has publicly disclosed [13].

Question: When may information from education records be disclosed?

Answer: In general, information derived from a student's education records may be disclosed only if: (1) it is "directory information;" (2) the student has consented to the disclosure; or (3) the law provides an exception that permits disclosure without the student's consent.

Question: What is "directory information"?

Answer: FERPA allows institutions to designate certain classes of information as "directory information" that may be released to anyone without a student's consent [14]. Directory information may (but is not required to) include such items as the student's name, address (local, permanent, and e-mail), telephone number (local and permanent), photograph, dates of attendance at the institution, major, degrees and awards received, participation in officially recognized activities and sports, and date and place of birth, as well as other information "that would not generally be considered harmful or an invasion of privacy if disclosed [15]." A student's social security number or any student identification number that could be used by itself, without a password, PIN, or other authenticating factor, to access educational records may not be designated as directory information [16]. An institution that wishes to make directory information available must first give its students an opportunity to "opt out" and block the release of their own directory information, usually by making a formal request to the institution's registrar's office [17]. Even if a student has chosen to block the release of directory information, the institution may nevertheless continue to disclose that student's directory information under any other exception that may be applicable or with the student's case-by-case consent.

Question: May information from student education records be shared with others on campus?

Answer: Yes. Under one of FERPA's many exceptions to the general prohibition against disclosure,

campus personnel are free to share information from student education records with other “school officials” who have “legitimate educational interests” in the information [18]. Each institution must define for itself who qualifies as a “school official” and what is a “legitimate educational interest” and give annual notice of its definitions to its students [19]. These definitions can be quite broad – “school officials” need not be limited to “officers,” or even to employees [20], and “legitimate educational interests” (much like “education records”) need not be limited either to “academic” interests or to instances that are beneficial to the student. The Family Policy Compliance Office (“FPCO”) [21], the office within the U.S. Department of Education charged with overseeing and enforcing FERPA, offers the following model definitions:

A school official is a person employed by the University in an administrative, supervisory, academic or research, or support staff position (including law enforcement unit personnel and health staff); a person or company with whom the University has contracted as its agent to provide a service instead of using University employees or officials (such as an attorney, auditor, or collection agent); a person serving on the Board of Trustees; or a student serving on an official committee, such as a disciplinary or grievance committee, or assisting another school official in performing his or her tasks.

A school official has a legitimate educational interest if the official needs to review an education record in order to fulfill his or her professional responsibilities for the University [22].
At institutions that follow these or similar models, an employee concerned that a student’s statements or behavior evidence a potential threat could – and should – share relevant information with the dean of students, the judicial affairs office, the campus counseling center, the campus law enforcement unit, or other appropriate “school officials” whose job it is to deal with such issues.

Question: May information from a student’s education records be disclosed to protect health or safety?

Answer: Yes. FERPA permits the disclosure of information from student education records “to appropriate parties, including parents..., in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the student or other individuals [23].” For example, if a student sends an e-mail to his resident assistant saying that he has just been diagnosed with a highly contagious disease such as measles, the institution could alert the student’s roommate, and perhaps others with whom the student has come in close contact, to urge them to seek appropriate testing and medical care [24]. Safety concerns warranting disclosure could include a student’s statements about suicide, unusually erratic and angry behaviors, or similar conduct that others would reasonably see as posing a risk of serious harm [25].

This exception does not authorize “knee-jerk” or (in most cases) “broadcast” disclosures [26], but an institution need not be absolutely certain that there is an imminent crisis before invoking the exception. Rather, it is enough that, based on the totality of circumstances and on the basis of the facts that are available at the time, there is a rational basis for concluding that there is a threat to health or safety. As long as an institution can meet this relatively minimal threshold, "the Department will not substitute its judgment for that of the....institution in evaluating the circumstances and making its determination." [27]

The institution has the same good faith discretion to determine to whom disclosure should be made. In general, and when reasonably possible, the initial disclosure should be made to professionals trained to evaluate and handle such emergencies, such as campus mental health or law enforcement personnel, who can then determine whether further and broader disclosures are appropriate. Depending on the particular circumstances, disclosure under this exception may be made to law enforcement, parents, threat assessment teams or professionals, individuals who may have information necessary to determine the extent of a potential threat (such as friends, roommates, and prior schools attended), and potential victims and their families. If the concerns are of a more urgent nature, school officials should immediately contact campus or local police. FERPA permits each of these communications.

An institution that makes a disclosure on the basis of this exception must keep a record of the nature of the

perceived threat and the parties to whom the disclosure was made [28].

Question: When may a college or university disclose information from a student's education records to the student's parent or legal guardian?

Answer: Once a student is in attendance at a postsecondary institution, all rights provided by FERPA rest with the student, even if the student is younger than 18 years old [29]. Education record information may therefore be disclosed to the parent of a college or university student only with the student's consent or in instances in which one of the exceptions to FERPA permits disclosure. In addition to the other exceptions discussed in this Note, two such exceptions specifically address communications to parents.

First, FERPA permits (but does not require) disclosures of any or all education record information to a student's parents if the student is their dependent for federal tax purposes [30]. To rely on this exception, the institution must verify the student's dependent status, normally either by asking the student for confirmation [31] or by asking the parents for a copy of the relevant portion of their most recent tax return [32].

Second, an institution may (but again is not required to) provide information to a parent or legal guardian regarding any violation of law or of an institutional rule or policy governing the use or possession of alcohol or a controlled substance, if the institution has determined that the student committed a disciplinary violation with respect to such use or possession and the student is under the age of 21 at the time of both the violation and the disclosure [33].

These exceptions, like the other FERPA exceptions, are independent of each other. Thus, an institution may notify parents about a 19-year-old student's underage drinking violations even if the student is not their tax dependent, and may likewise notify the parents of a 22-year-old student's drug violations if the student is their tax dependent. Similarly, the situation need not rise to the level of a health or safety emergency in order for either of these exceptions to apply.

Question: What about disclosing information from the student discipline process, either to others on campus or to other institutions?

Answer: FERPA expressly permits institutions to include in a student's education records appropriate information concerning disciplinary action taken against the student for conduct that posed a significant risk to the safety or well being of that student, other students, or other members of the community [34]. Such information may be disclosed to any "school officials" who have "legitimate educational interests" in the behavior of the student, and it also may be disclosed as appropriate under the health and safety emergency exception. FERPA also expressly provides that, for purposes of the health and safety emergency exception, the "appropriate parties" to whom disclosure may be made include teachers and officials at other institutions who have legitimate educational interests in the behavior of the student [35].

In a separate (and again independent) exception, FERPA further permits institutions to disclose to anyone the final results of a disciplinary proceeding conducted against a student who is an alleged perpetrator of a crime of violence or a nonforcible sex offense [36], if the institution determines as a result of that disciplinary proceeding that the student committed a violation of the institution's own rules or policies with respect to such crime or offense. Yet another exception permits institutions to disclose the final results of such a proceeding to the victim *regardless* of whether the alleged perpetrator was found to be in violation of the institution's rules or policies [37]. For purposes of these two exceptions, "final results" is limited to the name of the student who is an alleged perpetrator of a crime of violence, the violation found to have been committed, and any sanction imposed against the student by the institution [38].

Question: **Are there other circumstances in which a college or university may disclose information from student education records to another institution without the student's consent?**

Answer: In addition to the exceptions discussed above, FERPA expressly permits (but does not require) the disclosure of information from a student's education records to officials of other institutions at which the student seeks or intends to enroll or where the student is already enrolled, so long as the disclosure is related to the student's enrollment or transfer [39]. To take advantage of this exception, the institution must either inform its students generally, in its annual FERPA notice, of its practice of doing so [40], or make a reasonable attempt to notify the individual student that it has done so [41]. In either case, upon request, the institution also must provide the student with a copy of the disclosed records and give the student an opportunity for a hearing to challenge the content of the disclosed records [42].

Question: **Can a college or university get information such as disciplinary or mental health records from a student's high school records?**

Answer: Yes. Colleges and universities have several options for obtaining information from a student's high school records. They can ask students to consent to the disclosure of those records. Consent by the student would permit the high school to disclose the information. In addition, the college or university may ask the high school to disclose the student's records under an applicable FERPA exception, including the exception that expressly permits the disclosure of information from a student's education records to officials of other institutions at which the student seeks or intends to enroll or where the student is already enrolled, so long as the disclosure is related to the student's enrollment or transfer. Again, the prior institution may, but is not required by FERPA to, disclose information. The requirements of this exception are discussed more fully in the preceding question. A prior institution may also rely on the current institution's determination that there is a health or safety emergency and may disclose relevant information to the current institution under that exception [43]. State law may provide additional options for access to these records. For example, under Virginia law (Virginia Code Annotated § 23-2.1:3), colleges and universities "…may require that any student accepted to and who has committed to attend, or is attending, such institution provide, to the extent available, from the originating school a complete student record, including any mental health records held by the school. These records shall be kept confidential as required by state and federal law…" Finally, in appropriate circumstances, high school records may be obtained by a subpoena or court order.

The disclosure and protection of mental health records may also be subject to medical record privacy laws. The institution seeking these records should ensure that the records will be maintained with an appropriate level of confidentially once received to avoid misuse of the record or stigmatization of the student. Before considering a blanket requirement for the high school mental health and disciplinary records of all accepted or attending students, the college or university should be confident that it has adequate resources for the review of all of those records, and an appropriate protocol for responding to their contents and, as appropriate, permitting the affected students to respond.

Question: **Is the disclosure of campus law enforcement unit records restricted by FERPA?**

Answer: No. Records that are created by the campus law enforcement unit (whether commissioned police or non-commissioned security) at least in part for a law enforcement purpose are not "education records" and, at least as far as FERPA is concerned, may be shared freely with anyone the institution, in its discretion, deems appropriate [44]. For example, FERPA would not prevent a campus law enforcement unit from disclosing to external law enforcement agencies an incident report concerning the unit's response to a student's threatening statements or behavior. However, any copies of that report that are shared with other campus offices would become subject to FERPA, though the original in the law enforcement unit would

continue not to be [45]. Moreover, any student education records that other campus offices share with the campus law enforcement unit, as "school officials" with a "legitimate educational interest," remain subject to FERPA even in the hands of that unit [46].

Question: What if the institution receives a court order or subpoena requesting student records?

Answer: The institution may disclose records in response to a judicial order or lawfully issued subpoena but generally must notify the student of the order or subpoena before complying [47]. An exception to this general rule is that a federal grand jury subpoena or other subpoena issued for a law enforcement purpose may instruct the institution not to notify the student [48].

Question: May an employee disclose personal knowledge and impressions about a student, based on the employee's personal interactions with the student?

Answer: Yes. FERPA's disclosure restrictions apply only to information derived from student education records, not to personal knowledge derived from direct, personal experience with a student [49]. For example, a faculty or staff member who personally observes a student engaging in erratic and threatening behavior is not prohibited by FERPA from disclosing that observation. (If at some point the employee describes the observation in a personally identifiable record, that record would be subject to FERPA protections. The employee would still be permitted to disclose the personal observation but would not be permitted to disclose the record of the observation unless one of the exceptions to FERPA applied or the student consented to the disclosure). Again, however, the employee generally should limit disclosure of such information to professionals trained to evaluate and manage it, as other privacy laws conceivably could apply and prohibit broader disclosures, depending upon the circumstances.

Question: What other laws protect student privacy?

Answer: Students may have additional privacy rights under state privacy and confidentiality laws and under federal laws. The Department of Health and Human Services and the Department of Education have issued joint guidance on the application of FERPA and the Health Insurance Portability and Accountability Act ("HIPAA") [50] to student health records. This joint guidance confirms that the HIPAA privacy rule expressly excludes student health records maintained by colleges and universities [51]. Moreover, certain professionals on campus, such as medical and mental health care providers, may be bound by professional obligations of confidentiality that require a higher burden to be met (such as a *significant* threat of *serious* and *imminent* harm to a specifically *foreseeable* victim) before disclosure of information in their possession may be made. Even when this is the case, however, other personnel on campus (such as a faculty member, dean of students, or residential life employee) may disclose information about a student under the lower FERPA health and safety emergency standard if the circumstances warrant.

Question: What happens if I violate FERPA?

Answer: If an institution regularly violates FERPA, it runs the risk of losing its education-related federal funding. While thus far, the Family Policy Compliance Office (FPCO) has not revoked any institution's funding, it works with these institutions to get them to comply with the statute voluntarily.

FERPA does not give individuals the right to sue non-compliant institutions. But sometimes the unauthorized

disclosure of private information violates other laws, such as state medical confidentiality or privacy laws, which allow individuals to sue. Faculty and employees should consult campus counsel with questions about disclosing information in student records.

In the event of an emergency or serious concern about either campus safety or an individual's welfare, FERPA permits campus personnel to consult appropriate persons, including parents, if the information conveyed is necessary to protect the health or safety of the student or others. Any ambiguity about FERPA should be resolved in favor of disclosure, limited as necessary, to protect the safety of individuals.

Question: **What should a faculty member or other college or university employee do if he or she is concerned about a student?**

Answer: If the concern is that a student may engage in violent behavior, toward self or others, and the threat appears to be imminent, the employee should contact the campus police or security office immediately. If the concern is of a less urgent nature, or the employee is not quite sure what to make of a student's comments or conduct, the employee should consult with professionals on campus or associated with the institution, such as the Dean of Students, a campus counseling center, or law enforcement, who may be able to assess the potential threat, identify resources for the student, and provide information that could assist in deciding on an appropriate course of action. In consultation with appropriate campus resources, a collective decision may then be made to contact a family member, an appropriate off-campus resource, or others.

FERPA would not present an obstacle to any of these disclosures. The worst response is to ignore troubling or threatening behavior. School officials should trust their instincts when a student appears to be in trouble and should consult with others on campus.

CONCLUSION:

FERPA is not a serious impediment to the sharing of student information among campus officials or appropriate third parties when there is a legitimate concern relating to campus safety. Institutions may wish to review certain aspects of their current FERPA policies (such as what they include within the scope of "directory information," who they include as "school officials," and what they consider "legitimate educational interests") in order to gain maximum flexibility and discretion for information sharing. As important as maintaining current policies is the need to educate those on campus about the true limits and applications of FERPA. Finally, in the case of an emergency or serious threat to personal safety, any ambiguity about FERPA can – and should – be resolved in favor of protecting the safety of individuals.

FOOTNOTES:

FN1. 20 U.S.C. § 1232g.

FN2. 34 C.F.R. § 99.3 (definitions of "education records" and "record") and FPCO Letter to Richard J. Gaumer, Webber, Gaumer & Emanuel, P.C., January 31, 2007.

FN3. Disclosure of Anonymous Data Under FERPA, (FPCO letter to Matthew J. Pepper, Tennessee

Department of Education, November 18, 2004).

FN4. 34 C.F.R. § 99.3 (definition of "personally identifiable") and Disclosure of Information Making Student's Identity Easily Traceable (FPCO letter to Robin Parker, Miami University, October 19, 2004) and Disclosure of Education Records to Texas Office of Attorney General (FPCO letter to School District in Texas, April 6, 2006).

FN5. Unauthorized Access to Education Record Systems (FPCO letter to B. Alan McGraw, Altizer, Walk & White, October 7, 2005).

FN6. FPCO Letter to Diane Layton, Shelton State Community College, August 7, 1998.

FN7. Open Records Request (FPCO letter to Corlis P. Cummings, Board of Regents of the University System of Georgia, September 25, 2003).

FN8. Disclosure of Education Records to Legislative Audit Division (FPCO letter to Ardith Lynch, University of Alaska, May 23, 2005).

FN9. Disability Office Records (FPCO letter to David Cope, University of North Alabama, November 2, 2004).

FN10. FPCO Letter to Attorney for School District, October 31, 2003.

FN11. Trustees of Bates College v. Congregation Beth Abraham, 2001 WL 1671588 (Me. Super. Ct. Feb. 13, 2001).

FN12. Disclosure of Information About Juvenile Registered Sex Offenders (FPCO letter to W. Joseph Hatley, Lathrop & Gage, March 8, 2005).

FN13. FPCO Letter to Dr. Hunter Rawlings III, Cornell University, February 13, 2000. See also Status of education records and transcripts from public due process hearings (FPCO letter to Jerome D. Schad, Hudgson Russ, LLP, December 23, 2004).

FN14. 34 C.F.R. § 99.31(a)(11).

FN15. 34 C.F.R. § 99.3 (definition of "directory information").

FN16. 34 C.F.R. § 99.3.

FN17. 34 C.F.R. § 99.37.

FN18. 34 C.F.R. § 99.37(a)(1).

FN19. 34 C.F.R. § 99.7(a)(3)(iii).

FN20. Disclosure of Education Records to Outside Service Providers (FPCO letter to Jeanne-Marie Pochert, Clark County School District Legal Department, June 28, 2006).

FN21. "About the Family Policy Compliance Office".

FN22. "Model Notification Rights under FERPA for Postsecondary Institutions".

FN23. 34 C.F.R. § 99.36(a).

FN24. Disclosure of Immunization Records (FPCO letter to Martha Holloway, Department of Education, February 25, 2004) and Applicability of FERPA to Health and Other State Reporting Requirements (FPCO letter to Melanie P. Baise, The University of New Mexico, November 29, 2004).

FN25. School Official Using Access to Education Records without Legitimate Educational Interest; Limits of Health or Safety Emergency Exception (FPCO letter to J. Chris Toe, Strayer University, March 11, 2005).

FN26. Disclosure of Immunization Records (FPCO letter to Martha Holloway, Department of Education, February 25, 2004).

FN27. 34 C.F.R. § 99.36 (c).

FN28. 34 C.F.R. § 99.32 (a)(5).

FN29. 34 C.F.R. § 99.5 (a), 34 C.F.R. § 99.3 (definition of "eligible student") and Potential Conflict with State Law (FPCO letter to Omero Suarez, Grossmont-Cuyamaca Community College District, January 16, 2004).

FN30. 34 C.F.R. § 99.31(a)(8).

FN31. Model Form for Disclosure to Parents of Dependent Students and Consent Form for Disclosure to Parents.

FN32. Parents of dependent students, disclosure to (FPCO letter to Robert E. Bienstock, The University of New Mexico, October 29, 1993).

FN33. 34 C.F.R. § 99.31(a)(15)(i).

FN34. 20 U.S.C. §1232g (h). Of course, information about less serious offenses also may be recorded.

FN35. 34 C.F.R. § 99.36(b).

FN36. 34 C.F.R. § 99.31(a)(14).

FN37. 34 C.F.R. § 99.31(a)(13).

FN38. 34 C.F.R. § 99.39.

FN39. 34 C.F.R. § 99.31(a)(2).

FN40. For model language, see "Model Notification Rights under FERPA for Postsecondary Institutions".

FN41. 34 C.F.R. § 99.34(a)(1).

FN42. 34 C.F.R. § 99.34(a)(2) and (3).

FN43. 73 Fed. Reg. 74,806, 74,839 (Dec. 9, 2008).

FN44. 34 C.F.R. § 99.3 (part (b)(2) of the definition of "education records") and 34 C.F.R. § 99.8. See also Law Enforcement Unit Records (FPCO letter to Judith S. Bresler and Michael S. Molinaro, Reese & Carney, LLP, February 15, 2006).

FN45. 34 C.F.R. § 99.8(b)(2)(i).

FN46. 34 C.F.R. § 99.8(c)(2).

FN47. 34 C.F.R. § 99.31(a)(9)(ii) and Blanket Court Orders (FPCO letter to Monique C. Shay, Los Angeles County Office of Education, and Kelly Rozmus Barnes, Los Angeles Unified School District, March 28, 2006).

FN48. 34 C.F.R. § 99.31(a)(9)(ii)(A) and (B).

FN49. School Official Using Access to Education Records without Legitimate Educational Interest; Limits of Health or Safety Emergency Exception (FPCO letter to J. Chris Toe, Strayer University, March 11, 2005). This "exception" does not apply, however, if the employee gained the personal knowledge in the course of making an official determination that has been or will be recorded. For example, a faculty member who awarded a student a grade or a judicial affairs officer who suspended a student cannot disclose that information even though it is based on "personal knowledge". See FPCO Letter to Elvira Strehle-Henson, University of Colorado at Boulder, February 11, 2005.

FN50. Not all campus health providers are covered by HIPAA. For those that are, HIPAA expressly provides that it does not apply to records that are protected by FERPA.

FN51. Joint Guidance on the Application of the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to Student Health Records, November 2008.

AUTHORS:

Nancy E. Tribbensee

Steven J. McDonald

RESOURCES:

NACUA Resources:

Publications

- Christine R. Williams, *FERPA, GLBA & HIPAA: The Alphabet Soup of Privacy*, (2007).
- Nancy E. Tribbensee, *The Family Educational Rights and Privacy Act: A General Overview*, (2003).
- McDonald, Steven J., ed., *The Family Educational Rights and Privacy Act: A Legal Compendium*, Second Edition (2002).

Journal of College and University Law Articles

- "FERPA: Only a Piece of the Privacy Puzzle," by Margaret L. O'Donnell. 29 *Journal of College and University Law* 679 (2003).
- "FERPA and the Immigration and Naturalization Service: A Guide for University Counsel on Federal Rules for Collecting, Maintaining and Releasing Information About Foreign Students," by Laura Khatcheressian. 29 *Journal of College and University Law* 457 (2003).

Outlines

- "The Fundamentals of Fundamental FERPA," by Steven J. McDonald. *2009 NACUA Annual Conference.*
- "Student Privacy: From Facebook to FERPA," by Phyllis Karasov, Steven J. McDonald, and Margaret L. O'Donnell. *2006 NACUA Annual Conference Outline.*
- "Student Discipline: FERPA, Mental Health, Computers and Civility," by Nancy E. Tribbensee. *2006 NACUA Annual Conference Outline.*
- "The Family Educational Rights and Privacy Act," by Nancy S. Footer. *2004 NACUA Annual Conference Outline.*
- "Law Enforcement and College and University Computers," by Stephanie J. Gold. *2003 NACUA November CLE Workshop Outline.*
- "Attending to Students in Crisis: Duty to Warn of Potential Harm to Others, Duty to Protect Against Harm to Self, Duty to Prevent Suicide: Counseling Records – FERPA, HIPAA, Confidentiality," by Nancy J. Joyer and Kris Kaplan. *2003 NACUA Annual Conference Outline.*
- "Student Records in the Digital Age: Issues of Security, Privacy, and Maintenance," by Susan McKinney and Tina M.R. Falkner. *2003 NACUA Annual Conference Outline.*
- "FERPA: New Issues for Our Old Friend," by Steven J. McDonald and Barbara L. Shiels. *2002 NACUA Annual Conference Outline.*

Statutes and Regulations:

- The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g.
  - 34 C.F.R. Part 99 (Final Rule).
  - December 2008 Amendments to FERPA Regulations
- The Health Insurance Portability and Accountability Act, 42 U.S.C. §§ 1320d-1320d-8.
- Student Assistance General Provisions; Campus Safety, 59 Fed. Reg. 22314 (April 29, 1994) (final rule).
- Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. Parts 160 and 164.

U.S. Department of Education Resources:

- Family Policy Compliance Office (FPCO)
  - "About the Family Policy Compliance Office".
  - "Model Notification of Rights under FERPA for Postsecondary Institutions".
  - Disclosure of Information from Education Records to Parents of Postsecondary Students.
  - Parents' Guide to the Family Educational Rights and Privacy Act: Rights Regarding Children's Education Records.
  - Disclosure of Information from Education Records to Parents of Postsecondary Students.
  - Model Form for Disclosure to Parents of Dependent Students.
  - Model Form for Disclosure to Parents of Dependent Students and Consent Form for Disclosure to Parents.
  - Balancing Student Privacy and School Safety: A Guide to the Family Educational Rights and Privacy Act for Colleges and Universities
- FPCO Guidance Letters
  - Letter to Richard J. Gaumer, Webber, Gaumer & Emanuel, P.C., January 31, 2007.
  - Disclosure of Anonymous Data Under FERPA, (letter to Matthew J. Pepper, Tennessee Department of Education, November 18, 2004).
  - Disclosure of Information Making Student's Identity Easily Traceable (letter to Robin Parker, Miami University, October 19, 2004).
  - Disclosure of Education Records to Texas Office of Attorney General (letter to School District in Texas, April 6, 2006).
  - Unauthorized Access to Education Record Systems (letter to B. Alan McGraw, Altizer, Walk & White, October 7, 2005).
  - Letter to Diane Layton, Shelton State Community College, August 7, 1998.
  - Open Records Request (letter to Corlis P. Cummings, Board of Regents of the University System of Georgia, September 2003).
  - Disclosure of Education Records to Legislative Audit Division (letter to Ardith Lynch, University of Alaska, May 23, 2005).
  - Disability Office Records (letter to David Cope, University of North Alabama, November 2, 2004).
  - Letter to Attorney for School District, October 31, 2003.
  - Disclosure of Information About Juvenile Registered Sex Offenders (letter to W. Joseph Hatley, Lathrop & Gage, March 8, 2005).
  - Letter to Dr. Hunter Rawlings III, Cornell University, February 28, 2000.
  - Status of education records and transcripts from public due process hearings (letter to Jerome D. Schad, Hudgson Russ, LLP, December 23, 2004).
  - Disclosure of Education Records to Outside Service Providers (letter to Jeanne-Marie Pochert, Clark County School District Legal Department, June 28, 2006).
  - Disclosure of Immunization Records (letter to Martha Holloway, Department of Education, February 25, 2004).
  - Applicability of FERPA to Health and Other State Reporting Requirements (letter to Melanie P. Baise, University of New Mexico, November 29, 2004).
  - School Official Using Access to Education Records without Legitimate Educational Interest; Limits of Health or Safety Emergency Exception (letter to J. Chris Toe, Strayer University, March 11, 2005).
  - Potential Conflict with State Law (letter to Omero Suarez, Grossmont-Cuyamaca Community College District, January 16, 2004).
  - Parents of dependent students, disclosure to (letter to Robert E. Bienstock, University of New Mexico, October 29, 1993).
  - Law Enforcement Unit Records (letter to Judith S. Bresler and Michael S. Molinaro, Reese & Carney, LLP, February 15, 2006).
  - Blanket Court Orders (letter to Monique C. Shay, Los Angeles County Office of Education,

and Kelly Rozmus Barnes, Los Angeles Unified School District, March 28, 2006).
    - Letter to Elvira Strehle-Henson, University of Colorado at Boulder, February 11, 2005.

Cases:

- Jain v. State of Iowa, 617 N.W.2d 293 (Iowa 2000).
- Brown v. City of Oneonta, 106 F.3d 1125 (2d Cir. 1997).
- Trustees of Bates College v. Congregation Beth Abraham, 2001 WL 1671588 (Me. Super. Ct. Feb. 13, 2001).

Additional Resources:

- William Kaplin and Barbara Lee, *The Law of Higher Education* (Jossey Bass, 4th edition) (2006).
- American Association of Collegiate Registrars and Admissions Officers
    - FERPA Compliance
    - FEPRA Final Exam

Sample Institutional Training Resources:

- The Catholic University of America FERPA Reference Chart
- University of Maryland FERPA On-Line Tutorial
- University of Southern California FERPA On-Line Tutorial
- University of Puget Sound FERPA On-Line Tutorial
- University of North Texas On-Line FERPA Training
- George Mason University Student Privacy
- Arizona State University Student Privacy: Family Educational Rights and Privacy Act (FERPA)
- University of North Carolina at Charlotte FERPA Information and Forms
- North Carolina State University FERPA Forms
- The Family Rights and Privacy Act: 7 Myths — and the Truth by Steven J. McDonald. The Chronicle of Higher Education (April 18, 2008)

"To advance the effective practice of higher education attorneys for the benefit of the colleges and universities they serve."

Thank you for attending this event.

Today's event features an online, post-event evaluation form. To send us your feedback, please click on the link below, or type the URL into your web browser's address bar.

http://eval.krm.com/eval.asp?id=21868

Your feedback and comments are very important to us. Thank you in advance for taking the time to complete this evaluation!