

**Final Rule 34 CFR Part 99**  
**Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g**

The U.S. Department of Education issued the final FERPA regulations which formalized a number of changes as well as clarifications to the law regarding student education record privacy. The changes clarify disclosures in a health and safety emergency and allows them when there is a significant and articulable threat (that is later documented); re-define “attendance;” provide that a unique student identifier (but not an SSN) may be treated as directory information if the student cannot be personally identified; re-states the case law that an education record does not include grades on peer graded papers before they are collected and recorded by a teacher; reiterate earlier guidance on how to ascertain whether or not a student is a dependent;<sup>1</sup> state that prior consent is not required to disclose education records to an entity which outsources institutional services; and make clear that campuses put in each student's record the list of State and local educational authorities (as well as Federal) that may make further disclosure of the student's education record without consent. Final regulations are effective January 8, 2009.

Using the information template from the Department of Education<sup>2</sup>, below is a summary of the pertinent changes to the FERPA regulations:

### **§ 99.3 Definitions**

#### **Attendance**

The final regulations expand the definition of a student’s attendance (and thus covered by FERPA) by adding other situations in which students “attend” classes but are not physically present, such as distance learning: attendance by videoconference, satellite, Internet, or other electronic information and telecommunications technologies.

#### **Directory information**

Students must be informed of the kinds of information a campus designates as directory information and they must be given an opportunity to opt out of directory information disclosures. The statute and current regulations do not require any specific items to be directory information, allowing a campus to decide that for itself, but suggests the following: student’s name; address; telephone number; email address; photograph; date and place of birth; enrollment status; and major field of study.

#### **Social Security Numbers and student ID numbers**

The final regulations prohibit the disclosure of a student’s SSN as directory information; student ID numbers may be disclosed as directory information if they qualify as electronic identifiers; however, an institution may not disclose lists with these identifiers attached to students’ names, addresses, and other directory information and may not be used to post grades.

#### **Electronic personal identifiers**

Campuses may designate electronic personal identifiers as directory information, including student ID numbers, but only if the identifier functions essentially as a name and is not used by itself to authenticate identity. Similarly, it cannot be used by itself to gain access to education records - the identifier should be combined with other authentication factors known only to the user (such as a PIN).

---

<sup>1</sup> The campus may rely upon the student's assertion as to dependent status and the Education Department has developed a [model form](#) to assist in obtaining this information.

<sup>2</sup> <http://www.ed.gov/policy/gen/guid/fpco/pdf/ht12-17-08-att.pdf>

## **Disclosure**

This definition is expanded to allow a university to have access to information that it provided to the system or another institution without violating the statutory prohibition on redisclosure, 20 U.S.C. 1232g(b)(3). It will help deal with falsified transcripts, letters of recommendation, and other documents received by allowing an institution that has received a questionable document to return it to the “sender” for verification.

## **Post-enrollment records**

Records that pertain to an individual’s previous attendance as a student are “education records” under FERPA regardless of when they were created or received by the institution.

## **Peer-grading**

There is a new exception to the definition of “education records” that excludes grades on peer-graded papers before they are collected and recorded by a teacher. This clarifies that peer-grading does not violate FERPA.

## **§ 99.5 Disclosures to parents and rights of students**

The final regulations clarify that institutions may make education record disclosures to parents without the student’s consent under any of exceptions: to a parent of a dependent student under any circumstance; for any student: to a student’s parent under the alcohol or controlled substance exception (when found in violation of campus code prohibiting alcohol/drugs) or in connection with a health or safety emergency (as further discussed).

### **§ 99.31(a)(1) School officials.**

Institutions that allow “school officials, including teachers, within the agency or institution” to have access to students’ education records, without consent, must first make a determination that the official has “legitimate educational interests” in the information. The list of officials must be included in the annual FERPA notification.

### **§ 99.31(a)(1)(i)(B) Outsourcing**

The final regulations expand the “school officials” exception to include contractors, consultants, volunteers, and other outside service providers used by a university to perform institutional services and functions that the institution would otherwise provide with its own employees; this further requires that the list of such officials be included in the annual notification. Such outside service provider must be under the direct control of the disclosing institution and subject to the same conditions on use and re-disclosure of education records that govern other school officials. The institution may disclose education records without consent to its own law enforcement unit under the school officials’ exception but not to outside police officers.

### **§ 99.31(a)(1)(ii) Controlling access to education records by school officials**

Institutions are now required to use “reasonable methods” to ensure that instructors and other school officials (including outside service providers) obtain access to only those education records (paper or electronic) in which they have legitimate educational interests. Institutions are encouraged to restrict or track access to education records to ensure that they remain in compliance with this requirement. The higher the risk, the more stringent the protections should be (e.g., SSNs should be closely guarded).

### **§ 99.31(a)(2) Student’s new school**

An institution retains the authority to disclose and transfer education records to a student’s new school even after the student has enrolled and such authority continues into the future so long as the disclosure is for purposes related to the student’s enrollment/transfer.

After admission, the ADA does not prohibit institutions from obtaining information concerning a current student with disabilities from any school previously attended by the student in connection with an emergency and if necessary to protect the health or safety of a student or other persons under FERPA. A student’s previous school may supplement, update, or correct any records it sent during the student’s application or transfer period and may identify any falsified or fraudulent records and/or explain the meaning of any records disclosed previously to the new school.

### **§ 99.31(a)(6) Organizations conducting studies**

An institution may disclose personally identifiable information from education records, without consent, to organizations conducting studies “for, or on behalf of” the disclosing institution for predictive tests, student aid programs; or improving instruction once it has entered into a written agreement with the recipient organization that specifies that information from education records may only be used to meet the purposes of the study and must contain the current requirements in on re-disclosure and destruction of information. Campuses should either release de-identified information or remove students’ names and SSNs to reduce the risk of unauthorized disclosure of personally identifiable information.

### **§ 99.31(a)(9)(ii) Ex parte court orders under USA Patriot Act**

The USA Patriot Act authorizes the U.S. Attorney General (or designee) to apply for an *ex parte* court order that allows the AG to collect education records from an educational institution, without the consent or knowledge of the student or parent, that are relevant to an investigation or prosecution of an offense related to an act of domestic or international terrorism. The new FERPA regulations are consistent with this. The institution that is served by the AG with such an *ex parte* court order should ensure that the order is facially valid.

### **§ 99.31(a)(16) Registered sex offenders**

The Campus Sex Crimes Prevention Act created a new exception to the consent requirement in FERPA that allows institutions to disclose information concerning registered sex offenders provided under State sex offender registration and campus community notification programs. States must ensure that certain sex offenders register their name and address with the State authority where the offender lives, works, or is enrolled as a student. States are also required to release relevant information necessary to protect the public concerning persons required to register under what are known as “community notification programs.” Institutions must advise the campus community about where it can obtain information about registered sex offenders. An institution may disclose, without consent, information it has received from a State about a student who is required to register as a sex offender in the State.

### **§ 99.31(b) De-identification of information**

The final regulations provide objective standards under which institutions and State higher education authorities may release, without consent, education records, or information from education records, that has been de-identified through the removal of all “personally identifiable information.”

Under current regulations, **personally identifiable information** (PII) not only includes a student’s name and other direct personal identifiers (such as the student’s SSN or student number) but also indirect identifiers (e.g., name of the student’s parent; mother’s maiden name, the student’s or family’s address, and personal characteristics that would make the student’s identity easily traceable). They also add “biometric records” to the list of personal identifiers that constitute PII:

one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual, such as fingerprints, retina and iris patterns, voiceprints, DNA sequence, facial characteristics, and handwriting. The final regulations also clarify that an institution may not release information from education records if the requester asks for the record of a particular student, or if the institution has reason to believe that the requester knows the identity of the student to whom the records relate.

In releasing either redacted records or statistical information, a campus should also consider other information that might be linked to a student, (e.g., law enforcement records, published directories) and the cumulative effect of disclosure of student data. Make a determination about whether the other information that is linked or linkable to an education record would allow a “reasonable person in the school community” to identify the student “with reasonable certainty.” It is a matter of analyzing and balancing risk so that the risk of disclosure is very low.

### **§ 99.31(c) Identification and authentication of identity**

Under the final regulations, an institution must use reasonable methods to identify and authenticate the identity of parents, students, school officials, and any other parties to whom they disclose education records. Such authentication is complex for disclosure of electronic records but campuses may use personal security questions, biometric indicators, etc. and other factors known or possessed only by the user, as appropriate.

### **§ 99.33 Redisclosure of education records**

Current regulations prohibit recipients of education records, without prior written consent, from re-disclosing personally identifiable information from the records (unless prior, written understanding and under one of the exceptions).

### **§ 99.35(b)(1) By Federal and State officials**

Federal and State officials that receive education records for audit, evaluation, compliance and enforcement purposes may now re-disclose education records under the same conditions that apply currently to other recipients of education records, such as forwarding records to another official for another qualifying audit, evaluation, or compliance/enforcement purpose.

### **§ 99.33(b)(2) Under court order or subpoena**

The final regulations require a party that re-discloses education records on behalf of an educational institution in compliance with a court order or subpoena to comply with the parental notification requirements before it responds to the order or subpoena.

### **§ 99.33(c) Clery Act**

Under current regulations implementing the Clery Act in the HEOA, universities are required to inform the accuser and accused of the outcome of an institutional disciplinary proceeding brought alleging a sex offense. Previously, an institution could disclose the outcome of a disciplinary proceeding to a victim of a crime of violence or a non-forcible sex offense, regardless of the outcome, but only on the condition that the institution notify the recipient that he or she may not re-disclose the information without the student-perpetrator's consent. Now, disclosures under the Clery Act are not subject to the prohibition on re-disclosure and campuses may not require the victim to execute a non-disclosure or confidentiality agreement in order to receive information that the institution is required to disclose under the Clery Act.

### **§ 99.32 Recordkeeping requirements**

An educational institution does not have to maintain a record of re-disclosures but is now required to obtain a copy of the State or Federal official's record of further disclosures and make it available in response to a parent's or eligible student's request to review the student's record of disclosures.

### **§ 99.36 Health and safety emergencies**

In making a determination about making a disclosure under the health or safety exception, an institution may take into account the totality of the circumstances pertaining to a threat to the safety or health of the student or other individuals. If the institution determines that there is an articulable and significant threat to the health or safety of a student or other individuals, it may disclose information from education records to appropriate parties (including parents of an eligible student) whose knowledge of the information is necessary to protect the health and safety of the student or other individuals. The institution must record the articulable and significant threat that formed the basis for the disclosure and the parties to whom the information was disclosed. If there is a rational basis for the determination, the Department will not substitute its judgment for that of the institution in deciding to release the information. There is also clarification of the circumstances under which an educational institution may release, without consent, an eligible student's "treatment records" for purposes other than treatment.

### **§ 99.37 Directory information**

A campus may disclose “properly designated” directory information without written consent and permit students the opportunity to opt out before making such disclosures.

### **§ 99.37(b) Former students**

Institutions must continue to honor a former student’s opt-out request made while in attendance unless it has been specifically rescinded by the former student.

### **§ 99.37(c) Student identification and communication in class**

Opting- out of directory information disclosures does not prevent an institution from identifying a student by name or from disclosing his/her electronic identifier or institutional email address in class. This means that a student has no right to remain anonymous in class and may not impede routine classroom communications and interactions.

### **§ 99.37(d) Use of SSNs**

SSNs may not be used as an identification element when disclosing or confirming directory information unless the student has provided written consent for the disclosure. Without prior written consent of the student to confirm the SSN (for things like degree verification services), this implicit confirmation of the SSN is improper under FERPA.

### **§ 99.62, § 99.64, § 99.65, § 99.66, § 99.67 Enforcement Provisions**

The Family Policy Compliance Office (FPCO) has authority investigate an institution either when a parent or eligible student files a complaint or when it receives allegations from a university official or other party (including media reports) that FERPA has been violated. A complaint does not have to allege that an institution has a policy or practice of violating FERPA in order for the Department to investigate.

### **Safeguarding recommendations**

Although it is not required, the Department recommends notification to students about security breaches, such as inadvertent posting of students’ grades or financial information on publicly available Web servers; theft or loss of laptops that contain education records; computer hacking, etc. It encourages institutions to review publications such as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100, “Information Security Handbook: A Guide for Managers,” for guidance and to use any methods determined to mitigate the risk of unauthorized access and disclosure.

Institutions with questions are encouraged to consult with your own campus counsel.

Additional questions about how the final FERPA regulations affect our campuses may be sent to Kathryn Bender, Associate VP of Legal Affairs at [kbender@northcarolina.edu](mailto:kbender@northcarolina.edu).