

Rutgers Camden – Community Leadership Center

Family Educational Rights and Privacy Act (FERPA) and Research Implications¹

Overview: The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records. The law applies to all schools (i.e., elementary, secondary and higher education institutions) that receive funds under an applicable program of the U.S. Department of Education.

Summary of the FERPA Regulations: FERPA is a federal law that protects the privacy of personally identifiable information contained within a student's educational record. FERPA applies to all schools (K-12 including postsecondary institutions) that receive funds under various programs from the U.S. Department of Education.

FERPA defines educational records as records containing information (in any medium – paper, electronic, microfilm, etc.) that directly relate to a student and are maintained by an educational institution or by a party acting for the institution.

The information listed below is not considered part of an educational record and thus not regulated by FERPA; however, the information may be regulated or protected by other federal and state laws.

What Impact Does FERPA Have on Research?: FERPA impacts researchers in that data not included in the student directory information cannot be utilized in research without the permission of the IRB and the research participant. Keep in mind, however, that the IRB cannot overrule the institution's decision to deny access, and if the IRB disapproves the proposed research, the institution may not approve disclosure of information associated with the research.

Personally Identifiable Information:² The FERPA regulations require that educational agencies or institutions provide public notice to parents of students or eligible students of the types of personally identifiable information that are designated as directory information (34 CFR § 99.37). The parent or the eligible student must be given the right to refuse to have any or all of the student's information released as directory information. (An "eligible student" is a student who has reached 18 years of age or is attending a postsecondary institution (34 CFR § 99.3).

The definition of personally identifiable information is central to all discussions of privacy and confidentiality. The term 'personally identifiable information' refers to information that can be used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc." Personally identifiable information, as defined in FERPA, includes, but is not limited to:

1. The student's name;
2. The name of the student's parent or other family members;
3. The address of the student or student's family;

¹ Rutgers University - <https://orra.rutgers.edu/ferpa>

² <https://nces.ed.gov/pubs2011/2011601.pdf>

4. A personal identifier, such as the student's Social Security Number, student number, or biometric record;
5. Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;
6. 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;
7. Information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates. (34 CFR § 99.3)

Protecting Confidentiality Through De-Identification and Anonymization of Data³⁴: Other terms that are used in discussing confidentiality include de-identification and anonymization. These concepts are central to protecting against disclosures in data files that are shared with external education researchers. The term de-identified information is used to describe records that have enough personally identifiable information removed or obscured such that the remaining information does not identify an individual and there is no reasonable basis to believe that the information can be used to identify an individual. The FERPA 2008 regulations subsection on de-identified records allows for the nonconsensual release of student level information from education records, provided that

- (1) all personally identifiable information is removed
- (2) there is a reasonable determination that a student's identity is not personally identifiable. In making this determination, both single and multiple data releases from the education records should be taken into account along with other information available from other sources (34 CFR § 99.31(b)(1)).

Techniques described that can be used to protect student level data include generalizing the data by grouping continuous values and applying top and bottom coding to either continuous or categorical data to avoid outliers; suppressing the data by deleting entire records or parts of records; introducing "noise" into the data by adding small amounts of variation into selected data; swapping the data by exchanging certain data elements in one record with the same data elements from a similar record; blanking and imputing for randomly selected records; and blurring by replacing data with the average value by replacing a selected value (e.g., an outlier) of a data element with the average value for that data element for the entire group.

Techniques described to avoid disclosures in aggregate tabular data include establishing minimum cell sizes, suppression, complementary suppression, random rounding, controlled rounding, controlled tabular adjustment, and special rules to protect against disclosures that might include additional restrictions on publishing such as requiring results on more than one cell in a distribution, requiring certain size categories, and collapsing across categories.

Once a data file is de-identified, the FERPA regulations indicate that a re-identification code may be attached to the data file so that the file can be released for use for education research (34 CFR § 99.31(b)(2)). While the de-identified data file with a re-identification code does not provide external researchers with personally identifiable information about students, a

³ <https://nces.ed.gov/pubs2011/2011601.pdf>

⁴ <http://fpg.unc.edu/sites/fpg.unc.edu/files/resources/reports-and-policy-briefs/DaSyDeidentificationGlossary.pdf>

researcher is able to return to the source that issued the data to request additional data elements that can be added using the re-identification code. The re-identification code should be independent of any of the personally identifiable information. Only a limited number of staff should have knowledge of the method used to produce the code. Under FERPA, the re-identification code (1) may not be used for any purpose other than matching the de-identified records to the source to obtain additional information for education research; (2) may not be used to identify a student or personally identifiable information about a student; and (3) may not be based on a student's Social Security Number or other personal information (34 CFR § 99.31(b)(2)).

Anonymization takes the data one step beyond de-identification. That is, anonymized data are data that have been de-identified, and they do not include a re-identification code. In an anonymized data file, the student case numbers in the data records cannot be linked back to the original student record system. Returning to the examples discussed above, anonymized data would not be useful to staff using data to monitor the progress and performance of individual students. However, if a professor at a university reads the research report from the analysis of academic gains of students in the afterschool enrichment program and decides that he or she would like to have a class of graduate students apply different analytic procedures to see if the results can be replicated, an anonymized file could be produced from the de-identified file used by the researchers to serve this purpose. To do this, the re-identification code must be removed and the file should be reviewed to ensure that additional statistical disclosure techniques do not need to be applied. The documentation for the anonymized data file should identify any disclosure limitation techniques that were applied and their implications for the analysis.

What Information is Protected by FERPA?⁵

College Level:⁶

Certain kinds of student information fall under "directory-style information" (e.g., name, campus address, current credit load etc.) which means that this information can be obtained and used without IRB approval. Some kinds of student information (e.g., date of birth, GPA etc.) does not fall under student directory information and cannot be utilized in research without going through the proper channels. FERPA requires that students be given the option to "opt out" of allowing directly information to be shared, and if students choose to opt out, this information may not be disclosed.

Researchers need to receive consent from student research participants in order to utilize information that falls under FERPA's definition of education records (for definitions of "education record" or "records" please refer to 34 CFR 99.2 and/or 1232g(b)(3),(b)(5)(a)(4)). This includes

⁵ [Read More Information](#) [3] (ed.gov)

[Rutgers FERPA Info](#) [4]

[Rutgers FERPA Directory Info](#) [5]

⁶ Note: If the IRB grants the waiver of informed consent, a designated school official (at Rutgers- IRAP) must strip any personally identifiable information (PII) before the dataset will be shared with you (for a definition of the term "PII" please see federal regulations 34 CFR 99.3 or 20 U.S. Code 1232g). Examples of PII include – but are not limited to – student names, student identification numbers, grade lists, place of birth, ethnicity, course schedules, academic status, and advisor names. The waiver, however, does not absolve you of the responsibility to notify the students of the possibility to opt out of research project. Students retain this right to their educational records even if they no longer attend Rutgers (34 CFR 99.37).

– but is not limited to – end-of-course grades or any other grades or assignments produced within a class. In other words, instructors cannot use information to which they might have natural access for purposes other than instruction and evaluation without informed consent. Course grades are considered part of the students' official records and thus belong to the student, and permission of the student should be obtained through informed consent, along with permission of the Registrar. Other information not typically in a student directory could include race, gender, birthdate, GPA, country of citizenship, social security number, residency status, and financial aid (including PELL Grants or HOPE Scholarship) or academic status. This list, however, is not exhaustive.

Does this mean that I cannot use my students' grades or coursework in my research without IRB approval?

Yes, FERPA regulations apply even when using your “own” records and/or your “department’s” student records. Unless you have received a waiver ([see RU SOPs 5.10 Waiver of Informed Consent or consent process guidance \[2\]](#)), you must receive IRB approval **and** student consent in order to utilize any grades and/or work completed within your class, including assignments such as papers, journals, projects, and tests (34 CFR 99.2). In practical terms, this means that you will need to obtain student consent either by securing access to educational records contained in Rutgers's directory or – if this is not possible – by obtaining consent via established informed consent procedures.

Early Childhood through 12th grade level

FERPA applies to all research projects conducted within local PK-12 schools and school districts. The PI is responsible for obtaining IRB approval from Rutgers University, and s/he also needs to comply with any additional safeguards that have been put into place by individual school districts or early childhood programs.

Are there research projects involving access to data not typically included in student directory information that do not require informed consent from participants?:

Educational institutions may disclose, without consent, student data to those conducting studies for, or on behalf of, educational institutions to (1) develop, validate, or administer predictive tests; (2) administer student aid programs; or (3) improve instruction (34 CFR 99.31).

Educational records may be released, as well, for institutional research; however, individuals proposing to publish or publicly disseminate such research would need IRB approval before proceeding.

Irrespective of the consent route, however, student research participants need to be informed about the following three issues so they know what they are consenting to: (1) nature of records that will be disclosed/used, (2) the purpose of the disclosure, and (3) the identification of the part of class or parties to whom the disclosure may be made (34 CFR 99.30).

Conditions for Which Student Records Can Be Disclosed Without Consent: Generally, schools must have written permission from the student (or parent if the student is a minor) in order to release any information from a student's education record. However, FERPA allows schools to disclose educational records without consent under special circumstances.

The U.S. Department of Education's summary of the FERPA regulations lists the following conditions for which student records can be disclosed without consent:

- Develop, validated, or administer predictive tests;
- School officials with legitimate educational interest (e.g., improve instruction);
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies;
- State and local authorities, within a juvenile justice system, pursuant to specific state law