# APPENDIX A

## The Family Educational Rights and Privacy Act

## Guidance for Reasonable Methods and Written Agreements

*What is the Family Educational Rights and Privacy Act?*

The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g, is a Federal privacy law administered by the Family Policy Compliance Office (FPCO or Office) in the U.S. Department of Education (Department or we). FERPA and its implementing regulations in 34 CFR part 99 protect the privacy of students' education records and afford parents and eligible students (i.e., students who are 18 years of age or older or attend an institution of postsecondary education) certain rights to inspect and review education records, to seek to amend these records, and to consent to the disclosure of personally identifiable information from education records (PII from education records).

The general rule under FERPA is that PII from education records cannot be disclosed without written consent. However, FERPA includes several exceptions that permit the disclosure of PII from education records without consent. Two of these exceptions are discussed in this document – the studies exception and the audit or evaluation exception. The two exceptions contain specific, and slightly different, requirements, described more fully in the implementing regulations (34 CFR Part 99).

*What is the purpose of this document?*

The audience for this document includes schools, school districts (also referred to as local educational agencies (LEAs)), postsecondary institutions, and State educational authorities (such as State educational agencies (SEAs)) that may disclose PII from education records. Our intent is to provide these entities with information about requirements and best practices for data disclosures under the studies exception and the audit or evaluation exception.

*What is the Studies Exception? (see 20 U.S.C. §1232g(b)(1)(F) and §99.31(a)(6))*

The studies exception allows for the disclosure of PII from education records without consent to organizations conducting studies for, or on behalf of, schools, school districts, or postsecondary institutions. Studies can be for the purpose of developing, validating, or administering predictive tests; administering student aid programs; or improving instruction.

> Example: An SEA may disclose PII from education records without consent to an organization for the purpose of conducting a study that compares program outcomes across school districts to further assess what programs provide the best instruction and then duplicate those results in other districts.

*What is the Audit or Evaluation Exception? (see 20 U.S.C. 1232g(b)(1)(C), (b)(3), and (b)(5) and §§99.31(a)(3) and 99.35)*

The audit or evaluation exception allows for the disclosure of PII from education records without consent to authorized representatives of the Comptroller General of the U.S., the Attorney General, the Secretary of Education, and State or local educational authorities (FERPA-permitted entities). Under this exception, PII from education records must be used to audit or evaluate a Federal- or State-supported education program, or to enforce or comply with Federal legal requirements that relate to those education programs (audit, evaluation, or enforcement or compliance activity). The entity disclosing the PII from education records is specifically required to use reasonable methods to ensure to the greatest extent practicable that its designated authorized representative complies with FERPA and its regulations.

> Example: An LEA could designate a university as an authorized representative in order to disclose, without consent, PII from education records on its former students to the university. The university then may disclose, without consent, transcript data on these former students to the LEA to permit the LEA to evaluate how effectively the LEA prepared its students for success in postsecondary education.

*How do you define education program?*

"Education program" is an important term under the audit or evaluation exception because PII from education records can only be disclosed to audit or evaluate a Federal- or State-supported "education program," or to enforce or to comply with Federal legal requirements related to an education program. As specified in the FERPA regulations, §99.3, an education program must be principally engaged in the provision of education, including, but not limited to, early childhood education, elementary and secondary education, postsecondary education, special education, job training, career and technical education, and adult education, and any program that is administered by an educational agency or institution. For a definition of "early childhood program" please refer to §99.3 of the FERPA regulations.

*Do we need to have a written agreement to disclose PII from education records without consent?*

Yes. Both the studies exception and the audit or evaluation exception specifically require that the parties execute a written agreement when disclosing PII from education records without consent. The mandatory elements of that agreement vary slightly between the two exceptions.

*Are there mandatory provisions for written agreements under the studies exception?*

Yes. Written agreements under the studies exception must in accordance with the requirements in §99.31(a)(6)(iii)(C):

1. Specify the purpose, scope, and duration of the study and the information to be disclosed. Your agreement must specify the purpose of the study, describe its scope and its duration, and identify the information being disclosed.

2. Require the organization to use PII from education records only to meet the purpose or purposes of the study as stated in the written agreement. Your agreement must specify that the PII from education records must only be used for the study identified in the agreement.

3. Require the organization to conduct the study in a manner that does not permit the personal identification of parents and students by anyone other than representatives of the organization with legitimate interests. Your agreement must require the organization to conduct the study so as not to identify students or their parents. This typically means that the organization should allow internal access to PII from education records only to individuals with a need to know, and that the organization should take steps to maintain the confidentiality of the PII from education records at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques.

4. Require the organization to destroy all PII from education records when the information is no longer needed for the purposes for which the study was conducted, and specify the time period in which the information must be destroyed. Your agreement must require the organization to destroy the PII from education records when it is no longer needed for the identified study. You should determine the specific time period for destruction based on the facts and circumstances surrounding the disclosure and study. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit.

*Are there mandatory provisions for written agreements under the audit or evaluation exception?*

Yes. The mandatory provisions for written agreements under the audit or evaluation exception are similar to, but slightly different from, the provisions required for written agreements under the studies exception. Section 99.35(a)(3) specifically requires that the following provisions be included in written agreements under the audit or evaluation exception:

1. Designate the individual or entity as an authorized representative. Your agreement must formally designate the individual or entity as an authorized representative.

2. Specify the PII from education records to be disclosed. Your agreement must identify the information being disclosed.

3. Specify that the purpose for which the PII from education records is being disclosed to the authorized representative is to carry out an audit or evaluation of Federal- or State-supported education programs, or to enforce or to comply with Federal legal requirements that relate to those programs. Your agreement must state specifically that the disclosure of the PII from education records is in furtherance of an audit, evaluation, or enforcement or compliance activity.

4. Describe the activity with sufficient specificity to make clear that it falls within the audit or evaluation exception. This must include a description of how the PII from education records will be used. Don't be vague – the agreement must describe the methodology and why disclosure of PII from education records is necessary to accomplish the audit, evaluation, or enforcement or compliance activity.

5. Require the authorized representative to destroy the PII from education records when the information is no longer needed for the purpose specified. Your agreement should be clear about how the PII from education records will be destroyed.

6. Specify the time period in which the PII must be destroyed. Your agreement must provide a time period for destruction. You should determine the specific time period for destruction based on the facts and circumstances surrounding the disclosure and activity. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit.

7. Establish policies and procedures, consistent with FERPA and other Federal and State confidentiality and privacy provisions, to protect PII from education records from further disclosure (except back to the disclosing entity) and unauthorized use, including limiting use of PII from education records to only authorized representatives with legitimate interests in an audit, evaluation, or enforcement or compliance activity. The agreement must establish the policies and procedures, consistent with FEPRA and other Federal and State laws, to protect PII from education records from further disclosure or unauthorized use.

*Can an entity receiving PII from education records disclose it in a way that allows individual students to be identified?*

No. Absent consent from the parent or eligible student, FERPA provides that the PII from education records cannot be published in a way that would allow individual students and their parents to be identified. The organization conducting the study, audit, or evaluation can use PII from education records to conduct the study, audit, or evaluation, but results must be published in a way that protects the privacy and confidentiality of the individuals involved. For example, when publishing tables, cell suppression and other methods of disclosure avoidance can be used so that students cannot be identified through small numbers displayed in table cells.

*Under the audit or evaluation exception, what is your responsibility to use "reasonable methods" to ensure that your authorized representative is FERPA-compliant to the greatest extent practicable? (§99.35(a)(2))*

When you disclose PII from education records under the audit or evaluation exception, you are required to use "reasonable methods" to ensure to the greatest extent practicable that your authorized representative is FERPA-compliant. This specifically means ensuring that your authorized representative does the following:

1. Uses PII from education records only to carry out an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with, Federal legal requirements related to these programs. You should make sure that the proposed audit or evaluation is legitimate, and require in your written agreement that your authorized representative use the PII from education records only for that audit, evaluation, or enforcement or compliance activity. You should not disclose all of your PII from education records; rather, you should determine which specific elements your authorized representative needs and disclose only those.

2. Protects the PII from education records from further disclosures or other uses, except as authorized by you in accordance with FERPA. Your agreement must specify that your authorized representative may not further disclose the PII from education records, unless authorized. Approval to use the PII from education records for one audit or evaluation does not confer approval to use it for another.

3. Destroys the PII from education records when no longer needed for the audit, evaluation, or enforcement or compliance activity. Your agreement must specify that your authorized representative is required to destroy the PII from education records when it is no longer needed and specify the time period in which the PII must be destroyed.

*Are there best practices that support reasonable methods?*

Yes. While it is vital for organizations to comply with FERPA and its regulations, FERPA represents the floor for protecting privacy, not the ceiling. Accordingly, the Department is also specifying best practices, in which we describe actions we recommend you take to ensure that your authorized representative is protecting privacy to the greatest extent possible. Best practices are broader than FERPA compliance and describe recommended actions you should take to ensure that your authorized representative is FERPA-compliant to the greatest extent practicable.

These best practices may apply to data sharing under both the audit and evaluation exception and the studies exception. Please keep in mind that not all of the following best practices are appropriate in every instance, and this list does not include every possible protection. Before disclosing PII from education records under one of these exceptions, you should examine the following list and tailor your practices as necessary and appropriate.

- *Convey the limitations on the data.* You should take steps to ensure your authorized representative knows the limitations on the use of the data (i.e., that the data is only to carry out the audit or evaluation of Federal- or State-supported education programs, or to enforce or to comply with Federal legal requirements that relate to those programs).

- *Obtain assurances against redisclosure.* You should obtain assurances from your authorized representative that the data will not be redisclosed without permission, including such assurances that your authorized representative will provide you (the disclosing entity) the right to review any data prior to publication and to verify proper disclosure avoidance techniques have been used.

- *Be clear about destruction.* You should set clear expectations so your authorized representative knows what process needs to be followed for the proper destruction of PII from education records.

- *Maintain a right to audit.* You should maintain the right to conduct audits or other monitoring activities of your authorized representative's policies, procedures, and systems.

- *Verify the existence of disciplinary policies to protect data.* You may want to verify that your authorized representative has appropriate disciplinary policies for employees that violate FERPA. This can include termination in appropriate instances.

- *Verify the existence of a sound data security plan.* You may wish to verify before disclosing PII from education records that your authorized representative has a sound data security program, one that protects both data at rest and data in transmission. You have a responsibility to determine if your authorized representative's data security plan is adequate to prevent FERPA violations. The steps that you may need to take in order to verify a sound data security program are likely to vary with each situation. In some cases, it may suffice to add language to the written agreement that states what data security provisions are required. In other cases, it may be more prudent for you to take a hands-on approach and complete a physical inspection. Additionally, your written agreements could specify required data security elements, including requirements related to encryption, where the data can be hosted, transmission methodologies, and provisions to prevent unauthorized access.

- *Verify the existence of a data stewardship program.* You may want to examine your authorized representative's data stewardship program. Data stewardship should involve internal control procedures that protect PII from education records and include all aspects of data collection – from planning to maintenance to use and dissemination. The Department believes that a good data stewardship plan would have support and participation from across the organization, including the head of the organization, management, legal counsel, and data administrators, providers, and users. The plan should detail the organization's policies and procedures to protect privacy and data security, including the ongoing management of data collection, processing, storage, maintenance, use, and destruction. The plan could also include designating an individual to oversee the privacy and security of the PII from the education records it maintains. For more information, we have posted for comment a technical brief: "Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records" that can be found at http://nces.ed.gov/programs/Ptac/Toolkit.aspx?section=Technical%20Briefs.

- *Disclose only PII from education records that is needed.* When you consider disclosing PII from education records to an authorized representative for an audit, evaluation, or enforcement or compliance activity, you may want to explore which specific data elements are necessary for that activity and provide only those elements. You should take care to ensure that you are not disclosing more PII from education records than needed for the stated activity and purpose. You should also explore whether PII from education records is actually required, or whether de-identified data would suffice.

- *Know to whom you are disclosing data.* You may want to require your authorized representative to conduct background investigations of employees who will have access to PII from education records, or you may want to conduct these investigations yourself. Additionally, you may want to require your authorized representative to

disclose past FERPA or data management violations. If you discover past violations, you would want to explore the circumstances behind the violation, and discover all information that would allow you to make an informed judgment on whether the individual or entity is likely to be a responsible data steward. This may include discovering whether the violation was covered up, including if it was voluntarily reported to affected students or FPCO, and whether appropriate breach response procedures were followed.

- *Verify training.* You may want to verify that your authorized representative has a training program to teach its employees about FERPA and how to protect PII from education records, or you may want to train your authorized representatives yourself.

*Are there best practices for written agreements?*

You should consider the following items for inclusion in your written agreements for work under both the audit or evaluation exception and the studies exception. We note that this list may not cover everything you want in your agreement – you should look to the facts and circumstances surrounding the disclosure agreement and include all terms necessary to be clear about roles, responsibilities, and expectations for safeguarding PII from education records.

- *Bind individuals to the agreement.* It can be important to bind not just the entity to whom you are disclosing PII from education records, but also the individuals who will be accessing that data. There are several ways to accomplish this result. One way is to identify the individuals in the agreement itself, and have them execute the agreement in their individual capacity as well as having a representative execute the agreement for the entity. Alternatively, your agreement can require individuals accessing the PII from education records to execute affidavits of nondisclosure or other documentation indicating their individual agreement to handle the PII from education records properly.

- *Agree on limitations on use of the PII from education records.* Your agreement should be clear about limitations on the use of the PII from education records, meaning that it can only be used for the activities described in the agreement. Your agreement may also address methodological limitations, for example, identifying which data sets, if any, the PII from education records may be linked.

- *Agree to not redisclose.* The most basic provision of the agreement is to make clear that the PII from education records is confidential and must not be redisclosed through direct data disclosures or publishing results that allow individuals to be directly or indirectly identified. FERPA-permitted entities may wish to require that specified disclosure avoidance methodologies be applied, or may wish to review all results prior to publication, or both.

- *Specify points of contact/data custodians.* Your written agreements should specify points of contact and data custodians (the individuals directly responsible for managing the data in question).

- *Mention Institutional Review Board (IRB) review and approval.* While FERPA does not mention IRBs, research proposals involving human subjects may have to be reviewed and approved by IRBs, if required under protection of human subject regulations of the Department and other Federal agencies. If IRB review and approval is required or expected, this may be noted in the written agreement.

- *State ownership of PII from education records.* You may wish for your agreement to be clear that, in disclosing PII from education records to an entity, you are in no way assigning ownership of the PII or records to that entity, and that it may only be redisclosed with your permission or otherwise in compliance with FERPA and its regulations.

- *Identify penalties.* Your agreement could include penalties under State contract law such as liquidated damages, data bans of varying length, and any other penalties the parties to the agreement deem appropriate. You may want your agreement to create third-party beneficiary rights, e.g., allowing parties injured by a data breach to sue for damages. While FERPA itself has little flexibility for sanctions, you can include a wide range of appropriate sanctions in your written agreements.

- *Set terms for data destruction.* As discussed previously, written agreements for both studies and audits and evaluations are required to contain provisions dealing with the destruction of PII from education records when those records are no longer needed. The agreement could include a method for documenting the destruction, such as the use of notarized statements.

- *Include funding terms.* If the agreement involves cost reimbursement, these details could be specified.

- *Maintain right to audit.* You may want to include the right to conduct audits or otherwise monitor the entity to which you are disclosing PII from education records to periodically affirm that the entity has appropriate policies and procedures in place to protect the PII from education records.

- *Identify and comply with all legal requirements.* It is important to remember that FERPA may not be the only law that governs your agreement. The agreement could broadly require compliance with all applicable Federal, State, and local laws and regulations, and identify the legal authority (whether express or implied) that permits the audit, evaluation, or enforcement or compliance activity.

- *Have plans to handle a data breach.* While no one anticipates a data breach, data loss may occur. You may wish to include specific procedures in your written agreements detailing the parties' expectations in the event that PII from education records is lost, including specifying the parties' responsibilities with regard to breach response and notification and financial responsibility.

- *Review and approve reported results.* If applicable, the written agreement could specify the parties' agreements with respect to publication of results. For example,

you may wish to review and approve reports prior to publication to make sure that they reflect the original intent of the agreement.

- *Define terms for conflict resolution.* The agreement could specify procedures for how disputes between the parties would be resolved.

- *Specify modification and termination procedures.* The agreement could specify how it can be modified or terminated. You may wish to provide specific provisions for termination based on improper handling of PII from education records.

*What do I do if the terms of the written agreement are violated?*

If the entity to which you have disclosed PII from education records without consent (whether under the studies exception or the audit an evaluation exception) violates the terms of the written agreement, you should evaluate your options under the penalty and termination provisions of the agreement. You may want to stop disclosing PII from education records to that organization, or pursue legal redress. If you have reason to believe that the entity has violated FERPA, you should contact FPCO.

*How should the public be informed?*

It is a best practice to keep the public informed when you disclose PII from education records.

- *Inform the public about written agreements.* Transparency is a best practice. You might want to post your data sharing agreements on your Web site, or provide some equivalent method to let interested parties know what data you are disclosing, the reasons it is being disclosed, and how it is being protected. While the Department generally recommends public posting of written agreements, parties are encouraged to review their contractual data security provisions carefully and redact, prior to publication, any provisions that may aid those seeking unauthorized access to systems. In certain instances a separate confidential IT Security Plan may be appropriate. For more information on data security best practices, see the Privacy Technical Assistance Center (PTAC) Web site: http://nces.ed.gov/programs/ptac.

*Who should I call if I have questions?*

If you would like more information about best practices to protect PII from education records, contact the PTAC Help Desk at PrivacyTA@ed.gov or 855-249-3072.

If you are a parent, eligible student, school, LEA, or SEA and would like more information on FERPA, please call FPCO at 1-800-872-5327.