

11-1-2017

Ask and You Might Not Receive: How FERPA's Disclosure Provisions Can Affect Educational Research

Lindsey Tonsager

Covington & Burling LLP, ltonsager@cov.com

Caleb W. Skeath

Covington & Burling LLP, cskeath@cov.com

Follow this and additional works at: <https://ir.library.louisville.edu/jsfa>

Part of the [Higher Education Commons](#), and the [Higher Education Administration Commons](#)

Recommended Citation

Tonsager, Lindsey and Skeath, Caleb W. (2017) "Ask and You Might Not Receive: How FERPA's Disclosure Provisions Can Affect Educational Research," *Journal of Student Financial Aid*: Vol. 47 : Iss. 3 , Article 6.

Available at: <https://ir.library.louisville.edu/jsfa/vol47/iss3/6>

This Issue Article is brought to you for free and open access by ThinkIR: The University of Louisville's Institutional Repository. It has been accepted for inclusion in *Journal of Student Financial Aid* by an authorized administrator of ThinkIR: The University of Louisville's Institutional Repository. For more information, please contact thinkir@louisville.edu.

Ask and You Might Not Receive: How FERPA's Disclosure Provisions Can Affect Educational Research

By Lindsey Tonsager and Caleb W. Skeath

The Family Educational Rights and Privacy Act (FERPA) regulates how schools collect, use, and disclose student information, including disclosures to third-party educational researchers. This article examines how educational researchers can structure their activities to reduce the risk of violating FERPA's disclosure restrictions. In order to do so, we present two options for researchers to consider: utilizing de-identified student information that does not fall within the scope of FERPA, or complying with FERPA by securing prior consent for student information disclosure or qualifying for an exception from FERPA's consent requirement. The article's discussion of these options includes an overview of FERPA's legal framework, along with the practical advantages and disadvantages of each option.

Keywords: FERPA, disclosure, legal, student privacy, educational privacy, education record, consent, PII

As privacy becomes more of a focal point across different industries and sectors, the education sector is no exception. Schools, vendors, researchers, and other third parties have had to confront an increasingly complex matrix of laws and regulations governing the collection, use, and disclosure of student information. In this article, we examine how the primary federal law governing student data privacy, the Family Educational Rights and Privacy Act (FERPA), can affect the types of student data that educational institutions can disclose to researchers and the various options for obtaining student data in compliance with FERPA. We also discuss the application of several other legal frameworks that may govern the use and disclosure of certain types of financial aid data, such as the Higher Education Act (HEA) and the Privacy Act.

Within the United States, both state and federal privacy laws regulate the collection, use, and disclosure of student information. At the federal level, FERPA restricts how a school that receives federal funding can use and disclose student records. The HEA governs the use and disclosure of certain types of financial aid data, while the Privacy Act applies to the disclosure of records maintained by any federal agency, including the U.S. Department of Education. In addition to these federal laws, many U.S. states have passed laws or regulations that restrict the ability of schools or third parties to collect, use, or disclose student information. Researchers may also enter into contractual agreements with schools that restrict a researcher's ability to receive, use, or disclose student information. Depending on the information in question, it may be subject to multiple sets of legal requirements.

Lindsey Tonsager is a partner at Covington & Burling LLP. Caleb W. Skeath is an associate at Covington & Burling LLP.

At a bare minimum, schools will expect educational researchers to comply with FERPA's limitations on how schools can disclose students' personally identifiable information (PII) to third parties. Faced with these requirements, educational researchers have two options: (a) comply with FERPA's statutory requirements in order to obtain student information, or (b) use de-identified student information that is not subject to FERPA's requirements. The process of complying with FERPA can be onerous. It includes, in some cases, securing prior express written consent from parents or eligible students for the disclosure of student records, or complying with the strict limitations of one of several available FERPA exceptions. While using de-identified data allows researchers to avoid the logistical difficulties of FERPA compliance, it also restricts the level of detail present in the data, and possibly its usefulness in research.

This article will discuss the advantages and disadvantages of both options within the context of the U.S. legal framework for student data privacy. The article starts by providing background on the legal framework in the United States, including FERPA and the HEA, before discussing the advantages and disadvantages of working with identifiable student data within the FERPA framework versus using de-identified data.

Background

Within the realm of U.S. student data privacy law, FERPA is the most broadly applicable statute regulating the collection, use, and disclosure of student information. Depending on the source of the information in question, it may also be subject to the provisions of the HEA. While state laws and contractual terms may impose additional restrictions on the collection, use, and disclosure of student information, this article focuses on the restrictions imposed by FERPA as the most broadly applicable set of requirements, in addition to specific restrictions on financial aid data imposed by the HEA. In addition, researchers should evaluate any applicable state laws, local laws, or contractual requirements that may restrict what a researcher can do with student data.¹

FERPA

FERPA applies to any educational institution or agency, including a postsecondary educational institution, that receives federal funding (34 C.F.R. 99.3). In practice, FERPA casts a fairly broad net and subjects most postsecondary institutions to FERPA requirements, including any non-public institutions that receive federal funding. Even though these requirements only apply directly to the educational institution, the institution's compliance requirements affect how researchers and other third parties can obtain student information from the institution.

FERPA governs the use and disclosure of personally identifiable information in a student's education record. These terms are important in defining the scope of FERPA compliance obligations, so they are worth unpacking a bit further.

- An *education record* is a record that is (a) "directly related" to a student, and (b) maintained by an educational agency or institution, or a party acting on its behalf (34 C.F.R. 99.3).
- *Personally identifiable information (PII)*, in contrast, generally includes any 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

¹ A separate federal statute, the Protection of Pupil Rights Amendment, imposes parental notice and opt-out requirements on educational institutions under certain circumstances, including certain surveys or assessments of students that cover sensitive categories of information (such as political or religious beliefs) or gathering information for marketing purposes. The Privacy Act may also apply to data obtained from the U.S. Department of Education's databases, including the National Student Loan Data System.

the student with reasonable certainty (34 C.F.R. 99.3). It also includes information requested by a person who the educational institution reasonably believes knows the identity of the student to whom the education record relates. The FERPA regulations include some examples of such information, such as a student's name, the names of the student's parents or other family members, the address of the student or the student's family, the student's personal identifier (such as a Social Security number, student number, or biometric record), or "indirect identifiers" such as a student's date of birth, place of birth, or mother's maiden name.

In the absence of an applicable FERPA exception, an educational institution subject to FERPA may only disclose PII from an educational record to a third party with prior written consent from the parent or eligible student, as discussed in greater detail below.

Higher Education Act

While FERPA applies broadly to many types of student data, including student financial aid information, the HEA specifically governs the use and disclosure of certain sources of data gathered through student financial aid programs for postsecondary education. The restrictions imposed by the HEA vary depending on whether the data in question originate from one of three sources:

1. The Free Application for Federal Student Aid (FAFSA), the primary application method for postsecondary federal student financial aid;
2. The National Student Loan Data System (NSLDS), the U.S. Department of Education's centralized database for information regarding recipients of federal student financial aid; or
3. The Institutional Student Information Record (ISIR), a record generated by the U.S. Department of Education and provided to the school that contains the information reported on the student's FAFSA, the student's financial aid history from NSLDS, and key financial aid processing results.

This section focuses on restrictions imposed by two separate HEA provisions: Section 483(a)(3)(E), which applies to FAFSA or ISIR data, and Section 485B(d)(2), which applies to NSLDS data.

Under Section 483 of the HEA, data collected through the FAFSA or contained in an ISIR can only be used "for the application, award, and administration of" federal or state aid programs or aid awarded by eligible institutions (20 U.S.C. § 1090(a)(3)(E)). While financial aid research is unlikely to involve the application for or award of financial aid, certain types of research may qualify as administration of student aid programs governed by the HEA. The U.S. Department of Education has stated that the administration of student financial aid programs includes "audits and program evaluations necessary for the efficient and effective administration of these student programs" (U.S. Department of Education Privacy Technical Assistance Center [USDE PTAC], 2017, p. 6). If a researcher's work is aimed at promoting the efficient and effective administration of financial aid programs governed by the HEA, it may fall within the scope of data usage permitted under the HEA.

Section 485b of the HEA applies a different set of restrictions to NSLDS data. Under the HEA, non-governmental researchers or policy analysts cannot access PII from the NSLDS, and NSLDS data cannot be used for marketing purposes (20 U.S.C. § 1092b). According to the U.S. Department of Education, these restrictions apply not only to data obtained directly from the NSLDS, but also to NSLDS data provided through an ISIR (USDE PTAC, 2017). In addition, because the U.S. Department of Education maintains NSLDS, information obtained directly from the NSLDS may also be subject to the Privacy Act, as discussed below.

Other Legal Restrictions

In addition to FERPA and the HEA, researchers should also be aware of the Privacy Act, which requires written consent for the disclosure of information from databases controlled by the U.S. Department of Education or other federal agencies. A researcher attempting to access information from the NSLDS or other U.S. Department of Education databases should be prepared to comply with the Privacy Act's consent requirements or one of its exceptions that permits disclosure of certain types of information without consent (5 U.S.C. § 552a).

To assist with the interpretation of applicable federal laws, including FERPA, the HEA, and the Privacy Act, the U.S. Department of Education's Privacy Technical Assistance Center (PTAC) frequently releases guidance on best practices in complying with FERPA and other laws that may govern the use and disclosure of student information. Although this guidance is not binding, it is a good source of information about how the U.S. Department of Education interprets these requirements. Notably, PTAC has released the most definitive guidance to date on how the U.S. Department of Education views de-identification of student information (USDE PTAC, 2012).

More recently, PTAC has released guidance specifically addressing the use of financial aid information for research purposes. In this guidance, PTAC provided an overview of the applicable provisions of FERPA, HEA, and the Privacy Act, as well as PTAC's view of how these provisions apply to research activities. This guidance also contains a set of frequently asked questions that address whether certain types of sharing for research and evaluation purposes are permissible under applicable law (USDE PTAC, 2012).

Most states also have laws that govern the collection, use, and disclosure of student data. These laws can vary significantly by state and impose restrictions and requirements in addition to those provided by federal law. Researchers should consider whether any such restrictions may apply, usually depending on the state in which the educational institution providing the records is located.

Finally, an educational institution may seek to impose additional restrictions on its disclosure of student data by requiring recipients or users of the data to agree to contractual terms. Compliance with FERPA or state law does not automatically mean that you are complying with these terms. Researchers should review any such terms carefully prior to signing them to make sure that they can agree to the restrictions or requirements that the terms impose.

Option 1: Using De-identified Student Information

To avoid dealing with the burden of FERPA compliance, one common option is simply using de-identified information that does not fall under FERPA. Information qualifies as de-identified if it does not allow for the identification of a specific individual. Since this information no longer directly relates to a student, FERPA's restrictions on the use and disclosure of PII from education records do not apply.

De-identifying data may also alleviate some requirements imposed by the HEA. Although the HEA prohibits non-governmental researchers or policy analysts from accessing PII from the NSLDS, this prohibition should no longer apply to the disclosure of de-identified information from the NSLDS. Since the de-identified data no longer qualify as PII, the HEA should not restrict the ability of non-governmental researchers or policy analysts to access NSLDS data.

The use of de-identified information also comes at a practical cost, as the information is often less granular because it is devoid of data elements that constitute PII. It is possible to obtain individual-level de-identified information, but the only data elements left will be elements that are sufficiently indistinct so as to

not permit the identification of the student based on the data. Alternatively, for more sensitive categories of data that might allow for identification of a specific student, an educational institution may be able to disclose aggregate data or disclose data in ranges to reduce the risk that an individual student can be identified from the data set.

FERPA specifically contemplates the use of de-identified information for educational research purposes (34 C.F.R. 99.31(b)). Under FERPA, a parent's or eligible student's prior consent to the disclosure of student records is not required if the school removes "all personally identifiable information" from the records and makes a reasonable determination that the student's identity is not personally identifiable, whether through single or multiple releases of information, taking into account other reasonably available information. FERPA also allows schools to attach "record codes" to de-identified student-level data that the school releases for educational research purposes, which can allow a researcher to track the attributes of an individual student (or groups of students) without the ability to identify that student. The institution must not disclose any information about how it generates and assigns codes, and must not use any code that would allow for re-identification of a student (such as using part of a student's Social Security number as the code) or use the code for any other purposes.

PTAC has also released guidance on de-identification and other, similar techniques for removing PII from student information (USDE PTAC, 2012). While PTAC does not recommend a specific de-identification method, it does describe several possible methods, as well as concerns around de-identification that could lead to FERPA compliance issues. Notably, the PTAC guidance confirms that the removal of direct identifiers (such as name, Social Security number, or student ID number) is not sufficient to de-identify data. Instead, schools must consider how other data elements (such as grades, classes, aid amounts received, etc.) may be sufficiently unique to allow for the reasonable identification of an individual student, taking into account other information that may be publicly available (or that may be released in the future).

The PTAC guidance also encourages the use of "disclosure avoidance" techniques to minimize the risk of re-identification. These techniques include defining a minimum sample size and either combining data from individual students or suppressing unique data altogether. Subsequent PTAC guidance on the use of financial aid data for research clarifies that the de-identification process "typically requires" both removal of all direct and indirect identifiers along with the application of a disclosure avoidance technique such as suppression, recoding, or perturbation (USDE PTAC, 2017).

Although de-identification does relieve some of the logistical hurdles of complying with FERPA and the HEA while conducting research with student data, FERPA, the HEA, and PTAC guidance do not offer bright-line rules for what constitutes proper de-identification. As removal of direct identifiers is not enough, the school must also remove other data elements that could allow for re-identification of students (either due to small sample sizes or the public availability of other data that would allow for re-identification). Although these decisions should be made by the school prior to disclosing the data to the researcher, researchers should be aware that this process may impact the usefulness of the remaining data elements for research. Researchers who need unique, student-level, or more sensitive categories of information for research purposes may need to comply with applicable FERPA and HEA requirements to obtain student PII.

Option 2: Working within FERPA

If de-identified student data is not sufficient for researchers' needs, they may need to obtain student PII from the school. However, since FERPA governs the disclosures of student PII from the vast majority of schools, researchers should be aware of the restrictions imposed by FERPA and design research plans or

protocols to account for these restrictions. As noted above, FERPA requires prior written consent from a parent or eligible student for disclosure of PII in student records in the absence of an applicable exception. In addition to the consent requirement, this section will discuss two other potentially applicable exceptions: the school official exception and the directory information exception. Researchers should also be aware that even though prior written consent will permit the disclosure of student PII under FERPA, separate restrictions may still apply under the HEA.

Although FERPA allows the school to disclose student PII with the prior written consent of a parent or eligible student, this written consent must be signed and dated, and it must include the records to be disclosed, the purpose of the disclosure, and the party or class of parties to whom the disclosure may be made (34 C.F.R. 99.30). Electronic consent is also acceptable if it identifies and authenticates the person providing the consent and indicates that person's approval of the information contained in the electronic consent. A "parent" includes a guardian or an individual acting as a parent in the absence of a parent or guardian, while an "eligible student" is a student who has reached 18 years of age or is attending an institution of postsecondary education (34 C.F.R. 99.3).² Consent offers researchers the greatest latitude in terms of the ability to use (and disclose) the student information they receive. However, obtaining consent may impose significant logistical hurdles, in addition to creating potential issues if individual parents or students decide to withhold consent.

If a researcher does not or cannot obtain consent for a disclosure, FERPA does contain several exceptions that allow for the limited disclosure and use of student PII without consent. One such exception is the "school official" exception, which allows a school to disclose student PII without consent to a school official who has "legitimate educational interests" (34 C.F.R. 99.31(a)(1)). The school official can be a contractor, consultant, volunteer, or any other party to whom the institution has outsourced institutional services or functions, as long as the party

- Performs an institutional service or function for which the institution would otherwise use its own employees;
- Acts under the direct control of the institution with respect to the use and maintenance of education records; and
- Will not use the information for any purpose other than that for which the disclosure was made, and will not re-disclose the information without prior parent/student consent.

Unless the research in question is research that the school would perform itself, it is unlikely that the school official exception would apply to research-related disclosures. Even if it did apply, the school would have direct control over the use of the student PII it discloses, which may conflict with the goals of the researcher.

FERPA also allows schools to disclose "directory information" without consent. FERPA defines directory information to include information that, although it may constitute PII, is not generally "considered harmful or an invasion of privacy if disclosed" (34 C.F.R. 99.3). Under FERPA, directory information can include data elements such as a student's name; address; email address; telephone number; photograph; date and place of birth; major or field of study; grade level; enrollment status; dates of attendance; participation in officially recognized activities and sports; weight and height (for members of athletic teams); degrees, honors, and awards received; and the most recent educational agency or institution attended. However, directory information cannot include a student's Social Security number or (in most circumstances) student ID number.

² Once a student becomes an "eligible student," FERPA generally requires the prior written consent of the eligible student, not the parent, for disclosures of student PII. The parental rights provided by FERPA, including the rights to access and review education records, also transfer from the parent to the eligible student (34 C.F.R. 99.5(a)).

In order to disclose directory information, a school must provide an annual notice to parents and eligible students of the types of PII the institution has designated as directory information, the parents' or eligible students' right to opt out of disclosures of directory information, and the deadline for exercising this opt-out right. A school can also specify that it is only disclosing directory information to specific parties or for specific purposes, and must abide by these limitations if included. Under 34 C.F.R. 99.37(b), a school can disclose a former student's directory information without providing notice or an opportunity to opt out, but must continue to honor any valid request to opt out of these disclosures made while the student was in attendance at the school.

While a researcher could use directory information to support educational research, the availability of specific types of data could vary based on what types of data a school lists in its directory information disclosure notification, for what purposes (and to whom) a school states it will disclose directory information, and whether students or parents have opted out of directory information disclosures. In addition, certain data types, such as amounts of financial aid awarded, may be considered too sensitive to release as directory information.

Regardless of under which provision researchers obtain student PII, they should secure the information using "reasonable" security measures. Although FERPA does not provide significant detail on what might constitute reasonable security measures, it does emphasize the necessity of implementing reasonable measures to limit access to student information to individuals with a need to know. Researchers should also review applicable state law, contractual provisions, and general federal guidance in other substantive areas for indications as to other security practices that the U.S. Department of Education would expect a reasonable researcher to implement.

Researchers should also consider applicable restrictions under the HEA that may apply in addition to FERPA requirements. Most significantly, the HEA prohibits the disclosure of PII from the NSLDS to non-governmental researchers or policy analysts (20 U.S.C. § 1092b(d)(2)). The HEA also restricts the use of FAFSA and ISIR data to the administration of certain award programs, although this does permit "audits and program evaluations necessary for the efficient and effective administration of these student programs" (USDE PTAC, 2017).

Recommendations for Researchers

In collecting, using, and disclosing student information, educational researchers should structure their activities to reduce the risk of violating restrictions imposed by FERPA and similar legal frameworks such as the HEA and the Privacy Act. The following recommendations can help to guide appropriate use of student and parental data in research.

1. **Know what restrictions apply to which types of student information.** Although FERPA is the primary source of student data privacy restrictions in the United States, student data may be subject to multiple sets of restrictions from other federal laws, state laws, or contractual provisions. In addition to FERPA, the HEA also applies to FAFSA, NSLDS, or ISIR data, while the Privacy Act applies to data obtained from the U.S. Department of Education's record systems. Researchers should also carefully review any contracts or agreements that they enter into as part of receiving student information, and consider other state or federal laws that may apply to the collection, use, or disclosure of student information.
2. **Consider using de-identified information for research.** As FERPA does not apply to de-identified information, a school does not have to comply with FERPA in disclosing de-identified student information to researchers or other third parties. However, the de-identification process may

strip away many data elements necessary for effective research, making this approach impractical for certain research objectives.

3. **Consider operating within a FERPA exception.** Researchers who cannot use de-identified information to fulfill their research needs should consider whether they could qualify for the school official or directory information exceptions to FERPA's consent requirement. Each exception allows a school to disclose student information without obtaining consent, but both exceptions include restrictions that may make them a poor fit in certain research contexts.
4. **Determine logistics for obtaining consent, if needed.** If neither de-identified information nor FERPA exceptions provide the necessary student information, researchers should determine how they can satisfy FERPA's consent requirements and what legal requirements may still apply under the HEA or other laws even after they have secured consent. Although FERPA applies directly to schools, a school might seek to shift part or all of this compliance burden onto a researcher requesting access to student information. Examples of considerations include questions such as these: Will the researcher ask parents and eligible students to consent to the disclosure, or will the school ask? How will the researcher handle distributing and collecting consent forms? What will the researcher do if a parent or eligible student refuses to consent?

References

Family Educational Rights and Privacy Act, 34 C.F.R. Part 99 *et seq.* (1974).

Higher Education Act, 20 U.S.C. §§ 1090 and 1092b (1965).

Privacy Act, 5 U.S.C. § 552a (1974).

U.S. Department of Education, Privacy Technical Assistance Center (2012, October), *Data de-identification: An overview of basic terms*. Retrieved from http://ptac.ed.gov/sites/default/files/data_deidentification_terms.pdf

U.S. Department of Education, Privacy Technical Assistance Center (2017, January), *Guidance on the use of financial aid information for program evaluation and research*. Retrieved from http://ptac.ed.gov/sites/default/files/FSA_final.pdf