DATA INNOVATION PROJECT

Issue Brief: What Data-Informed Organizations Need to Know About Protected Education Data

Working with protected education data must be done thoughtfully but it is not insurmountable.

Framing the Challenge

Non-profit organizations are increasingly encouraged to incorporate strategic decision-making that is grounded in robust data. When trying to access data regarding educational outcomes, however, researchers and data stakeholders often come up against many challenges related to the requirements of the Family Education Rights and Privacy Act or FERPA. The goal of this issue brief is the help researchers and data stakeholders understand what FERPA actually says about privacy, what data are actually protected, solutions for accessing protected information, and where to go for additional guidance.

What is FERPA?

The Family Educational Rights and Privacy Act (FERPA) 20 U.S.C. § 1232g; 34 CFR Part 99) was established in 1974 and pertains to both K-12 educational records as well as post-secondary educational records. The purpose of FERPA is to provide parents, legal guardians and "eligible" students (that is, those over 18 years old attending a post-secondary institution) with the right to inspect files and request corrections, as well as ensure the privacy of those records. It is important to note that once a student turns 18 all rights under the act belong solely to the student, not his or her parents/legal guardian regardless of financial independence status. Privacy is protected by requiring schools to obtain individual consent for the disclosure of personally identifiable information from education records. A school must annually notify eligible students in attendance of their rights under FERPA.

Directory information is a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. Schools can release directory information without explicit consent, although they must notify parents, legal guardians and students about directory information annually and give them the opportunity to opt out of sharing this information. All other information is protected and may only be released with explicit, signed consent from the legal guardian (for students under age 18) or the eligible student. However, there are exceptions to this rule; schools may disclose records without violating FERPA to the following persons or when such conditions apply:

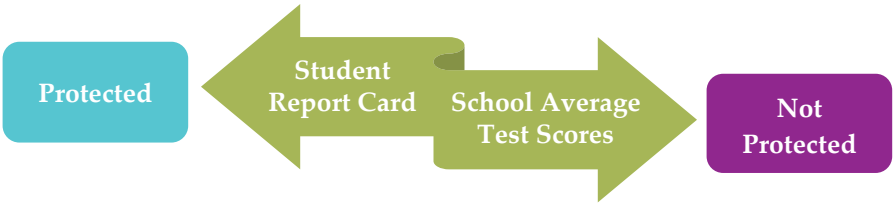
- School officials with legitimate educational interest
- Other schools to which a student is transferring
- Specified officials (e.g., local or state educational authorities, U.S. Attorney General) for audit or evaluation purposes
- Appropriate parties in connection with financial aid to a student
- 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

Educational records are directly related to a student and are maintained by an educational agency or institution or a party acting for or on behalf of the agency or institution. For example, grades, transcripts, class lists, student course schedules, health records (at the K-12 level), student financial information (at

the postsecondary level), and student discipline files are all considered educational records. The information may be recorded in any format including handwritten and printed documents, computer files, video files, audio files and e-mail.

Accessing Aggregate Reports

Personally identifiable information protected by FERPA exists when we can link an individual student to his or her educational record. Identifying information alone, such as personal names, residential addresses, or phone numbers, are not protected. The aggregation of student-level data into school-level reports protects educational records; although developed from individual student records, such reports do not identify any individual students and there is no reason to believe they could be used to identify an individual student. In this way, a report card is considered protected information, whereas average test scores for a school or grade are not.



To be considered "de-identified," **aggregate counts must be sufficiently large to ensure that individuals cannot be identified.** This becomes more difficult when researchers or data stakeholders request counts broken down by demographics or other characteristics. For example, imagine a researcher or data stakeholder asked a school for a report of average test scores by grade and student race. If the school released a report where any of the categories contained just one student, then the test score, grade, and race of that student has been accidentally disclosed. It is also important to note that accidental disclosure can also occur if all students in an easily observable group share a common characteristic that is reported (e.g., 100% of boys entering kindergarten were screened and deemed 'not school ready').

This challenge can be addressed by suppressing information that does not meet a minimum reportable count threshold. While a uniform threshold has not been established, statisticians consider three to be the absolute minimum needed to prevent disclosure, although larger minimums (e.g., 5 or 10) are typical. Other techniques to minimize accidental disclosure when working with aggregate reporting include rounding, reporting percentages or ranges (without the underlying numbers) or collapsing categories (e.g., examining racial groups as white/non-white).[1]

Accessing Protected Educational Records

To obtain data from educational records beyond directory or aggregate information, researchers and data stakeholders have three options, listed below. Each option also poses some challenges which are summarized in Table 1.

1. Obtaining written consent for each individual whose records will be accessed.
2. Obtaining de-identified data from the school (that is, identifying information has been removed by an authorized school official prior to releasing data to the researcher).
3. Claiming they are exempt from FERPA pursuant to the exceptions noted on page 1. For research purposes, the two most relevant exceptions are:
    - School officials with ***legitimate educational interest*** [34 CFR 99.31(a)(1)]
    - Organizations conducting certain ***studies for or on behalf of the school*** [34 CFR 99.31(a)(6)]

[1] Disclosure Avoidance, Privacy Technical Assistance Center (PTAC). http://ptac.ed.gov/sites/default/files/FAQs_disclosure_avoidance.pdf

Table 1. Considerations for Accessing Individual Educational Records

Access Strategy	Considerations
Obtaining written consent from each individual	May not be realistic given the number of students and/or legal guardians. Must be documented.
Obtaining de-identified data[2]	Schools may lack capacity (resources or knowledge) to sufficiently de-identify data records.
Invoking a FERPA exception	Must meet the expectations for the exception and secure data sharing agreement.

The phrases 'school officials' and 'legitimate educational interest' are not clearly articulated by FERPA and schools have the right to define each more specifically; however, FERPA does require schools to disclose their official definitions as part of the annual notification requirement. There are some generally accepted definitions provided by the U.S Department of Education. ***School officials*** typically include teachers, principals, administrative staff (including human resources, internet security and clerical), presidents or chancellors, board members, registrars, admissions officers, attorneys and accountants. Consultants or other professionals covered by a service provision contract are also often included. A school official has a ***legitimate educational interest*** if the official needs to review an education record in order to fulfill his or her job responsibilities, whereas curiosity or simply being a school or university employee does not satisfy this requirement. This means that an educator who has routine access to student records might not have a legitimate educational interest to conduct research with those records.

Studies on behalf of the school must be only for the purpose of developing, validating, or administering predictive tests; administering student aid programs; or improving instruction. Exceptions must be documented in writing and come from a school district's superintendent, or the University Registrar, depending on the records being requested. In addition, a written agreement with the organization specifying the purposes of the study and the use and destruction of the information is required.

Securing a Data Sharing Agreement

It is important for schools and educational institutions to ensure that researchers and data stakeholders are held accountable for protecting student records. Under FERPA, schools and institutions must secure a data sharing agreement with a researcher or data stakeholder before releasing individual records. The agreement should contain the purpose of the data, justification for the research, research plans, the data elements to be shared, how and when the data records will be destroyed in accordance with the law, and all the terms or conditions around further release or reporting of the data. A data sharing agreement should also be accompanied by a personal access agreement signed by the recipient stating that he or she agrees to be responsible for protecting the confidentiality of the records. Should the terms of the agreement change, including the timeline for destroying records, the data sharing agreement should be updated.

Destroying Educational Records

Data destruction means making paper files unreadable (e.g., shredding, blacking out) and digital files irretrievable (e.g., permanently deleted). FERPA does not contain requirements for schools about destroying protected information that they collect and maintain themselves, except that they must protect it from unauthorized disclosure and it cannot be destroyed if there is any outstanding review request. When a school or educational institution releases protected information to a researcher or data stakeholder, however, the data sharing agreements must specify that the information be destroyed when

[2] For detailed guidance on de-identification, please see Data De-identification: An Overview of Basic Terms. Privacy Technical Assistance Center (PTAC). May 2013. http://ptac.ed.gov/sites/default/files/data_deidentification_terms.pdf

it is no longer needed for the specific purpose outlined in the agreement. The agreement must also include a timeline for when files will be destroyed (e.g., within one month of study completion). FERPA does not provide any guidance on how to best destroy records.

Important Considerations

As a researcher or data stakeholder, it is important to weigh the costs and benefits of pursuing protected education information. Ask yourself whether you actually need that detailed level of information, and what it will provide to your research or quality improvement activities. How much effort will it take to satisfy the protections laid out in this issue brief? It is also important to explore whether there is another way to get meaningful information without requesting protected information; for example, through aggregate school reports that already exist (or that might need moderate tweaks), or by accessing existing surveillance data (e.g., public education repository or survey).

Conclusion

Educational data from schools and educational agencies contain a wealth of information about the overall well-being of a student community. This issue brief has described the various avenues by which researchers and data stakeholders can access educational records according the rules laid out by FERPA. Although carefully protected, using this information to inform research and data-driven quality improvement efforts is not insurmountable. The key takeaways around this issue are as follows:

- Aggregate data and data stripped of individual identifiers are not covered by FERPA and require no individual privacy protections but should be protected from accidental disclosure.
- Educational records may be used and disclosed for research with an individual's written permission.
- Educational records may be used and disclosed for research without consent in limited circumstances.

However, it is worth noting that other federal, state or local privacy regulations may dictate additional expectations to schools and how they handle student records; for example, the Health Insurance Portability and Accountability Act (HIPAA) and the Individuals with Disabilities Act (IDEA). Researchers and data stakeholders should work with schools to understand all the privacy requirements to which they are beholden.

References and Additional Resources

National Forum on Education Statistics. (2014). *Forum Guide to Supporting Data Access for Researchers: A Local Education Agency Perspective*. (NFES 2014-801). U.S. Department of Education. Washington, DC: National Center for Education Statistics. https://nces.ed.gov/pubs2014/2014801.pdf

Privacy Technical Assistance Center http://ptac.ed.gov

U.S. Department of Education http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html