New York State Senate
Standing Committee on Education

Public Hearing: The Regents Reform Agenda: Assessing Our Progress
October 1, 2013 - Syracuse City Hall, 233 East Washington Street, Common Council Chambers

Written Testimony of Reginal J. Leichty, Partner, EducationCounsel and Nelson, Mullins, Riley and Scarborough, Washington, D.C.

Good morning, my name is Reg Leichty, and I am a partner with EducationCounsel and the law firm Nelson, Mullins, Riley, and Scarborough in Washington, D.C. EducationCounsel is a mission based firm that supports the work of education leaders to close achievement gaps and improve education outcomes from pre-K through college.

Thank you for inviting me to be part of this public hearing about the Regent's education reform agenda. My testimony today focuses on the need to balance valuable state and local strategies for using data to improve education, with the important goal of ensuring student privacy and confidentiality. Specifically, my testimony will focus on the primary federal law designed to protect the privacy rights of students and their families, the Family Educational Rights and Privacy Act or FERPA.

Effective and appropriate data use by teachers, parents, school leaders and policy makers plays a critically important role in promoting learning. Provided with the right facts and tools, teachers can better tailor and individualize instruction, parents can monitor and support their children's educational progress, school and district leaders can identify and address program performance gaps and make better management decisions, and state leaders can assess the effectiveness of important state education reforms, like those underway in New York. These valuable and appropriate educational uses, however, must be carefully balanced by concerted state and local efforts to protect student privacy and confidentiality, including ensuring compliance with FERPA and adhering to data confidentiality and security best practices.

States and localities have a strong moral and legal obligation to respect and protect the privacy and confidentiality of students' personally identifiable information. At the federal level, personally identifiable student data protection is primarily governed by FERPA. The law imposes vitally important limits on the disclosure of student records by educational agencies and institutions that receive funds from the U.S. Department of Education. The law also provides parents with the right to inspect and challenge the contents of their children's educational records.

I would like to begin by providing a high level overview of FERPA's key requirements and conclude by making several recommendations for state leadership in this area. The recommendations represent suggestions for helping New York discuss and develop a sound strategy for ensuring data privacy and confidentiality, while also enabling teachers, parents, and state and local leaders to appropriately use data to promote better outcomes for all students.

Now more than ever, appropriate data use is critically important to educators' efforts to improve student achievement and close persistent achievement gaps. With the right strategy and policies in place, the educational opportunities created by innovative data systems can be maximized, while also protecting student privacy. The first step in designing such an approach, however, is developing a clear understanding of the very strong student privacy protections provided by federal law.

Family Educational Rights and Privacy Act Overview

First, FERPA prohibits sharing of students' personally identifiable information (PII), except in limited circumstances. PII includes – but is not limited to – obvious identifiers such as a student's name, address, social security or student number, or other information that alone or in combination would enable a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainly. PII also includes information requested by a person who the educational agency institution reasonably believes knows the identity of the student to whom the education records relates. Non-personally identifiable data, however are not covered by the law and may be shared without restriction. For example, educational agencies and institutions may, without limit, disclose aggregate, anonymous, and de-identified information derived from student records.

Second, FERPA's PII sharing exceptions are very limited and focused on promoting sound educational or public safety purposes. For example, PII may be shared for the purpose of: (1) evaluating state and local education programs and implementing school and district accountability; (2) conducting studies to improve instruction for or on behalf of an educational agency or institution; (3) providing records to a student's new or prospective school; (4) monitoring and analyzing assessment, enrollment, and graduation rates, and (5) enabling school officials, including contractors, on a need to know basis, to provide educational services. PII may also be shared with appropriate persons in order to protect the health or safety of the student or other persons in connection with an emergency. Under no circumstances may data be sold.

Third, the U.S. Department of Education's regulations balance these PII sharing exceptions, with requirements to protect student privacy and enforce the law. For example, the Department of Education's FERPA regulations require:

- authorized data holders to protect the data and destroy the records when no longer needed for authorized purposes. Specifically, state or local educational agencies must use "reasonable methods" to ensure "to the greatest extent practicable" that any individual or entity designated as its authorized representative to receive data to conduct evaluations, audits, or compliance activities: (1) uses student data only for authorized purposes; (2) protects the data from further disclosure or other uses; and (3) destroys the data when no longer needed.

- educational agencies and covered institutions to enter written agreements with authorized users to protect student data. Written agreements must be in place to establish privacy safeguards between the state or local education authority and the authorized representative to which it provides data to carry out evaluations, audits, or compliance activities. Such agreements must specify (among other things) who the authorized representative is, the information to be disclosed; and the activity to be carried out (with enough clarity to demonstrate that it comes within a purpose authorized by the law); provide for the destruction of the data when no longer needed for the authorized purpose, and establish policies and procedures to protect the data from further disclosure and unauthorized use.

- education agencies and covered institutions to deny further access to protected data if a violation occurs. Covered agencies or institutions must deny authorized representatives further access to PII for five years if the Department of Education's Family Policy Compliance Office (FPCO) determines that the representative has improperly disclosed data. Additionally, education agencies and other recipients of federal education funds are subject to investigations and enforcement, including possible withholding of funds for FERPA violations.

If FPCO finds a violation, however, it must give the noncompliant agency or institution an opportunity to come into voluntary compliance before taking any enforcement action, including actions to withhold funds and actions to debarring third-party agency or institutions from receiving further student data.

Issues for State Consideration

New York leaders should take steps to ensure that teachers, parents, school leaders and other decision makers have access to the data they need to ensure the best possible educational outcomes for students. The state should also, however, take appropriate steps to ensure that personally identifiable student data is protected and secure. This important step includes carefully adhering to FERPA and data management best practice. With this balanced goal in mind, I recommend that the state focus on three core areas:

- **Establishing appropriate roles for data stewardship.** Defining and clearly communicating authority, responsibility and accountability for decision making, management, and security of data.

- **Ensuring comprehensive policy documentation, public transparency and strong enforcement.** This step includes documenting laws, policies, and decisions related to data governance and communicating policies and procedures in a way that is accessible to stakeholders, including agency staff, students, parents and the public

- **Supporting organizational capacity building.** This step includes ensuring the state has the capacity and resources to implement and sustain these policies and procedures, including staff and technical system infrastructure.

In conclusion, I respectfully urge you to ensure that officials and individuals responsible for protecting student data utilize a coherent strategy and framework for guiding appropriate data use and oversight. This approach includes clearly justifying data collection, storage, and use for valid purposes, limiting access to personally identifiable information for educational purposes on a need to know basis, protecting data from inappropriate use, implementing a security framework, and providing public and parental notice about data collection, policies, access and use.

Thank you again for inviting me to testify on this important topic. I look forward to responding to your questions.