U.S. Department of Education
Safeguarding Student Privacy

The use of data is vital to ensuring the best education for our children. However, the benefits of using student data must always be balanced with the need to protect students' privacy rights. Students and their parents should expect that their personal information is safe, properly collected and maintained and that it is used only for appropriate purposes and not improperly redisclosed. It is imperative to protect students' privacy to avoid discrimination, identity theft or other malicious and damaging criminal acts. All education data holders must act responsibly and be held accountable for safeguarding students' personally identifiable information – from practitioners of early learning to those developing systems across the education continuum (P-20) and from schools to their contractors. The need for articulated privacy protections and data security continues to grow as Statewide Longitudinal Data Systems (SLDS) are built and more education records are digitized and shared electronically. As States develop and refine their information management systems, it is critical that they ensure that student information continues to be protected and that students' personally identifiable information is disclosed only for authorized purposes and under the circumstances permitted by law. All P-20 stakeholders should be involved in the development of these statewide systems and protection policies.

High quality data and robust data systems will help us measure our progress towards President Obama's goal for us to be first in the world in college completion by the year 2020 and better meet the needs of parents, teachers, and students. Whether we are referring to data collected by a State in aggregate form or student-level data stored by a school – we all share responsibility for those data, and how they are accessed and used in a secure manner that protects students' privacy and confidentiality. The current and proposed Family Educational Rights and Privacy Act (FERPA) regulations are a critical piece of this effort; however, it is equally important to consider that FERPA does not address the full scope of policies and procedures that should be in place to adequately protect student privacy in today's world of evolving technology and information use. As such, the U.S. Department of Education (Department) has begun several initiatives to provide technical assistance to States, districts, and schools to protect the privacy rights of students, promote the responsible use of data to inform education policy and practices and empower parents, teachers and students to use this information to advocate for their rights and improve their educational outcomes. Underlying all of the privacy initiatives of the Department are the Fair Information Practice Principles (FIPPs). The FIPPs were originally developed in 1973 by the predecessor agency of the Department, the U.S. Department of Health, Education, and Welfare. The FIPPs embody the core tenets underlying all privacy policies implemented by the Federal government from the Privacy Act to FERPA, from the Fair Credit Reporting Act to the Children's Online Privacy Protection Act and so on. As currently outlined by the Federal Trade Commission, the FIPPS include: notice/awareness, choice/consent, access/participation, integrity/security and enforcement/redress.

Each of the Department's initiatives emphasizes the need for all holders and users of data to understand their responsibilities under the law. The Department recognizes the important role the public has in driving this conversation to ensure that proper safeguards are in place to adequately protect the privacy of the Nation's citizens and its students. As such, the Department welcomes feedback on our efforts as described below.

Administration-Wide Privacy Efforts

The Department's work to safeguard students' personal information is part of a broader commitment throughout the Obama Administration to protect individual privacy. Efforts are underway across the Federal Government to protect privacy in areas such as commercial data, identity management, and cybersecurity.

The Department actively participates in the Administration's activities, serving on the National Science and Technology Council's Subcommittee on Privacy and Internet Policy and working with the National Science Foundation to lead the Formal Cybersecurity Education track of the National Initiative for Cybersecurity Education (NICE). The mission of NICE is to establish an operational, sustainable and continually improving cybersecurity education program that promotes the use of sound cyber practices that enhance the security and privacy of our citizens. The Department is helping to lead the track of NICE that aims to bolster formal cybersecurity education in pre-kindergarten through 12th grade, in post-secondary education and in career and technical education programs. It focuses on the science (including computer science), technology, engineering and math (STEM) disciplines to produce an enhanced "pipeline" of skilled professionals and workers in the cybersecurity disciplines for both the private sector and government. The Department will continue to play an active role in Administration-wide efforts to protect privacy.

Chief Privacy Officer

The Department has hired its first Chief Privacy Officer. Kathleen Styles joins the Department from the U.S. Census Bureau where she most recently served as Chief of the Office of Analysis and Executive Support. In that role she managed a portfolio that included confidentiality, data management, the Freedom of Information Act (FOIA), privacy policy and coordination for the acquisition and management of data from other agencies. She has extensive experience with Federal data collections, including the decennial census, and with ensuring appropriate protections for large databases. Ms. Styles holds a J.D. from William and Mary and a bachelor's degree from the University of Virginia. She is a member of the Texas and District of Columbia bars, and has practiced law in both the Federal sector and private practice. In addition to legal training, Ms. Styles is certified in government information privacy.

As Chief Privacy Officer, Ms. Styles oversees a new division at the Department dedicated to advancing the responsible stewardship, collection, use, maintenance and disclosure of information at both the national level and for States, local educational agencies (LEAS), postsecondary institutions and other education stakeholders. Her office will help to ensure that the Department complies with applicable legal obligations and epitomizes the best practices we espouse. It will work with other Department offices to include privacy, confidentiality and data security requirements in Department policies and programs; coordinate the development and delivery of privacy training for all Department employees and contractors; oversee the Department's retention and disposition of records; coordinate the development of official Department guidance for the education field on topics such as data stewardship, electronic data security and statistical methods for data protection; serve on the advisory board that manages the work of the Privacy Technical Assistance Center; and enforce the following statutes: FERPA, the Protection of Pupil Rights Amendment (PPRA), the Military Recruiter provision of the Elementary and Secondary Education Act of 1965, as amended (ESEA), the Privacy Act of 1974, as amended, and FOIA.

Privacy Technical Assistance Center

The Department has established a Privacy Technical Assistance Center (PTAC) which serves as a one-stop resource for the P-20 education community on privacy, confidentiality and data security. PTAC is a resource for State educational agencies (SEAs), LEAs, the postsecondary community and other parties engaged in building and using education data systems. It is based out of the National Center for Education Statistics (NCES) and its work is overseen by the Privacy Advisory Committee, which, in addition to the Chief Privacy Officer is comprised of senior leadership from other areas of the Department, such as NCES, the Office of the Chief Information Officer, the Family Policy Compliance Office, the Office of the General Counsel, and the Office of Planning, Evaluation and Policy Development.

PTAC's role is to provide timely and accurate information and guidance about data privacy, confidentiality, and security issues and practices in education; disseminate this information to the field and the public; and provide technical assistance to key stakeholders. PTAC will share lessons learned; provide technical assistance in both group settings and in one-on-one meetings with States; and create training materials on privacy, confidentiality and security issues. PTAC will accomplish its mission by providing the services and materials described below.

- **A "Privacy Toolkit" –** The toolkit will include a list of FAQs; a library of commonly-cited resources related to data privacy, confidentiality and security; checklists of important items to include in data governance plans and data security plans; FERPA guidance developed by the Family Policy Compliance Office; SLDS Technical Briefs (discussed below); and short issue briefs on key privacy topics. The toolkit will be available online as well as distributed at conferences and through mailed thumb drives. This toolkit will be the cornerstone of the information that PTAC will provide to education agencies to use in developing a roadmap to ensure better safeguarding of information, that data are used responsibly and that all who have access to it are held accountable for its proper use and security.

- **Technical Assistance Site Visits –** PTAC will conduct technical assistance site visits to different SEAs annually to offer in-depth reviews of SEA data policies and practices to provide recommendations for how to tackle that SEA's specific governance, technological or other challenges relating to privacy, confidentiality and data security.

- **Training Materials –** PTAC's experts will develop training materials for use by education stakeholders that offer real-world examples of how to develop longitudinal data systems that allow for effective data exchange while still protecting privacy, securing data from unauthorized access and ensuring the proper governance protocols are in place. PTAC will also offer the trainings online through Webinars, and will make the materials available at regional meetings and national conferences.

- **Help Desk –** The PTAC help desk is a centralized location for education stakeholders to submit questions to the Department on privacy, confidentiality and data security issues. The process for submitting questions to PTAC involves calling a toll-free number, emailing or mailing a question.

- **Regional meetings –** Each year, PTAC will host four one-day regional meetings to share training materials with SEAs, LEAs, institutions of higher education (IHEs), early childhood education programs, and/or workforce staff.

PTAC will regularly update its resources to reflect legal or policy changes as well as lessons learned from the field. For more information on PTAC or to submit questions, please refer to its website at: http://nces.ed.gov/programs/ptac/.

National Center for Education Statistics Technical Briefs

NCES has been working on a new series of technical briefs that further the national conversation on the best practices for overall data stewardship, which include data security and privacy protections related to SLDS. The methods in the briefs incorporate NCES statistical expertise with best practices from the field and consider various Federal data privacy laws, including, but not limited to FERPA. The technical briefs are intended to serve as fundamental resources for practitioners to consider adopting or adapting to complement the work they are already doing. These best practices are presented as voluntary methods and not a one-size-fits-all solution; it is essential that each institution's data policies account for all applicable Federal, State, local and tribal laws, as well as its community's needs.

For example, the Data Stewardship Technical Brief covers some best practices for managing personally identifiable information in electronic student education records. It recommends that educational agencies implement a privacy and data security program to protect personally identifiable information in electronic records and establish rules for permitted uses of that data. This brief explains that these policies and procedures are best developed by a data governance committee which would, among other things: lead the effort to inventory all personally identifiable information the organization collects and maintains, including how the information is used and who has access to it; determine if all personally identifiable information elements in the inventory are necessary and allowable to be collected and maintained; establish processes that verify the accuracy, completeness and age of the information elements maintained in the inventory; determine the sensitivity of each inventoried element and the risk of harm if that information was improperly disclosed; and set appropriate internal controls to restrict access to the data to only authorized users who have legitimate needs. In addition, the brief describes that it is necessary to inform the public regarding the existence of data systems that house personally identifiable information, explain what data elements are included in such a system and detail the public's right to review and appeal the contents of their individual records within that system. The best practices brief does not comment on the specifics of policies that should be implemented or how current procedures should be adjusted; it is expected that practitioners will implement data governance strategies that reflect the Federal and State requirements and best practices tailored to the local needs and laws of that community.

NCES has already released the following three briefs:

- Basic Concepts and Definitions for Privacy and Confidentiality in Student Education Records;
- Data Stewardship: Managing Personally Identifiable Information in Electronic Student Education Records; and
- Statistical Methods for Protecting Personally Identifiable Information in Aggregate Reporting.

The technical briefs can be accessed online at http://nces.ed.gov/programs/ptac/TechnicalBriefs.aspx. NCES plans to release at least four more technical briefs in 2011, covering the topics of Electronic Data Security, Data Access for External Researchers, Data Sharing across Sectors and Training.

We seek public input on the briefs, as they serve as a way to begin a conversation among the various early learning, elementary and secondary, postsecondary, and workforce agencies and institutions within the States. This feedback will inform the national conversation on these critical topics, which will ultimately result in better resources for education stakeholders and better guidance emerging from the Department. The Chief Privacy Officer will use the technical briefs, public feedback and additional input solicited from the education field as well as from privacy, technology and security experts to develop the Department's non-regulatory guidance on these topics that will complement the final FERPA regulation.

The Department encourages the public to review these resources as they become available and to direct comments to: SLDStechbrief@ed.gov.

Family Educational Rights and Privacy Act Notice of Proposed Rulemaking

The Department has also released a Notice of Proposed Rule Making (NPRM) outlining proposed amendments to its regulations implementing FERPA. Over time, interpretations of FERPA have complicated valid and necessary disclosures of student information without increasing privacy protections and, in some cases, dramatically decreased the protections afforded students. As States develop their longitudinal data systems, the Department has been informed of significant confusion in the education field surrounding what are permissible disclosures of personally identifiable student information from education records. This

confusion has led to delays in developing these systems or States proceeding in ways that may ultimately jeopardize student privacy. It was imperative for the Department to propose clarifying amendments to the FERPA regulations to ensure that these systems are being developed in ways that would allow States to meet the requirements of the American Recovery and Reinvestment Act of 2009 and the America COMPETES Act of 2007 and that do not put individual privacy at risk or create significant regulatory burdens. In addition, the NPRM proposes to expand who the Department may take enforcement actions against for improper redisclosure of student information and to clarify how directory information policies can be developed in ways that would provide greater protections to the privacy of student information and to the safety of students.

FERPA is a Federal law that protects the privacy of personally identifiable information from student education records. As the law applies to personally identifiable information contained in students' records, it is generally not applicable to other data that a school may collect, such as information on teachers (although there may be other State laws guiding the use and disclosure of that data). The law applies to all educational agencies and institutions, such as schools, school districts, and postsecondary institutions that receive funds under any program administered by the Department. Generally, schools must have written permission from the parent or eligible student in order to disclose any personally identifiable information from that student's education record. (An "eligible student" is a student who is 18 years old or attending a postsecondary institution at any age.)

FERPA permits, but does not require, schools to disclose personally identifiable information from education records without consent under limited circumstances, commonly known as *exceptions*. See § 99.31 for the full list of exceptions to the consent requirement in FERPA. In addition to proposed changes to the enforcement provisions in FERPA, the NPRM proposes to provide additional information and clarity, as discussed in more detail below, on three of those limited exceptions to the general consent rule: (1) the directory information exception; (2) the audit or evaluation exception; and (3) the studies exception. While the Department strongly encourages those who control student data to proactively notify parents and eligible students prior to disclosing personally identifiable information from the student's education records, this is not always feasible. Nonetheless, when an exception to the general consent requirement in FERPA applies, specific information **must be** recorded in the student's file that describes what information was disclosed and to whom it was provided. In addition, a parent or eligible student must be able to obtain information on these disclosures by reviewing the student's education record.

The NPRM is published in the *Federal Register* with a public comment period of 45 days. We encourage all interested parties to submit comments. Comments may be submitted through www.regulations.gov. Elements of the proposed regulations are discussed below. The full NPRM can be found at www.ed.gov/fpco.

Highlights of the Proposed Changes in the NPRM Consist of:

Stronger Enforcement

The Department needs stronger, more specific and clearer enforcement authority against all entities that collect, receive or maintain FERPA protected data. Every entity that receives personally identifiable information from student education records has a responsibility to ensure that it is used only for authorized purposes, is protected appropriately and is not redisclosed unless permitted by FERPA.

The Department's current regulations only discuss the application of the enforcement process to educational agencies and institutions which have students in attendance. Consequently, the NPRM proposes that if an entity (which does not have students in attendance) that receives Department funds violates FERPA, the Department may bring an enforcement action against that entity. Because State data systems are under the

control of the SEA, it is especially necessary to ensure that FERPA's enforcement remedies apply directly to SEAs by including SEAs in the definition of an educational agency or institution for purposes of enforcement.

The NPRM proposes expanding the types of entities that are subject to the enforcement provisions to include SEAs, LEAs, postsecondary agencies, and any other entity that is the recipient of Department funds, such as nonprofit organizations, student loan guaranty agencies and student loan lenders. If the proposed changes in the NPRM are finalized, these entities would be subject to enforcement proceedings if they violate applicable FERPA provisions which may include, but are not limited to the following:

- Proposed written agreement requirement that would be applicable to State and local educational authorities permitting them to redisclose personally identifiable information from students' education records to organizations under the studies exception and a similar proposed written agreement requirement that would be applicable to State and local educational authorities designating an authorized representative, other than an employee, under the audit or evaluation exception (discussed below);

- Proposed requirement for State and local educational authorities to use reasonable measures to ensure that their authorized representatives appropriately use, protect and destroy the personally identifiable information (discussed below);

- Redisclosure recordkeeping requirements; and

- Requirements to return or destroy data that are applicable to organizations to which personally identifiable information from education records is disclosed to conduct studies under the studies exception and to authorized representatives of State and local educational authorities to which personally identifiable information from education records is disclosed to evaluate or audit education programs (discussed below).

The applicability of these requirements depends on which exception to consent the entity is using to obtain access to or make further disclosures of personally identifiable information from education records. Entities that do not have students in attendance but receive personally identifiable information under a FERPA exception would not be required to comply with the annual notification provision in FERPA or permitted to designate directory information. In addition, any personally identifiable information that these entities collect and maintain that are separate from the student's education record maintained by an educational agency or institution are generally not subject to FERPA. For example, a student loan guaranty agency may receive personally identifiable student data from a university that originated from the student's education file under the exception to FERPA for student aid administration. This data would be subject to FERPA. However, data that is subsequently collected by the guaranty agency directly from the student would not typically be covered by FERPA, but may still be subject to other applicable Federal, State, local or tribal laws.

Ensuring the Safety of Students

Schools must have the flexibility to implement directory information policies that reflect their specific needs and policies without endangering students or opening the door for abuses of that information by allowing schools to limit the use of directory information.

FERPA defines "directory information" as information contained in an education record of a student that would generally not be considered harmful or an invasion of privacy if disclosed. Directory information may include elements such as the student's name, address, telephone number, photograph, date of birth, place of birth, grade level or major field of study. If a school has a policy of disclosing directory information, it is required to give annual public notice to parents and eligible students of the types of information designated as directory information and of the right to opt out of having a student's information so designated.

The NPRM proposes making two changes to the directory information exception with the goal of providing additional privacy and safety measures to protect students. The first proposed change would allow an educational agency or institution to specify in its annual public notice to parents and eligible students that disclosures of directory information may be limited to specific parties, for specific purposes or both. Many institutions have decided to forego designations of any directory information as they have concluded that such designations would put students at risk of becoming targets of marketing campaigns, the news media or even victims of criminal acts. These institutions then carry the burden of having to obtain consent for any use of the student's information, including more mundane uses such as yearbooks or graduation programs. A limited directory information policy would provide educational agencies and institutions the flexibility to designate directory information for more common uses without exposing their students to the risks of having their information released far more broadly.

The second proposed change would clarify that parents or eligible students may not prevent an educational agency or institution from requiring a student to wear or present a student ID or badge. The need for educational agencies or institutions to implement measures to ensure the safety and security of students should not be impeded by a parent or student using FERPA's directory information opt out provisions.

Ensuring the Effectiveness of Publicly Funded Programs
Connecting K-12 and Postsecondary Data and Sharing Information to Improve Early Childhood and Workforce Programs

States and local communities must have the ability to share student data to evaluate the effectiveness of education programs ranging from early childhood through adult education. In order to evaluate the effectiveness of their own education programs, States, school districts and high schools must be able to obtain college access, persistence, completion and remediation data on their former students from the postsecondary institutions that those students attend. School districts should be able to share student data with a local Head Start program so the Head Start program can evaluate whether its children were prepared to enter kindergarten ready to learn. Similarly, as States invest more resources preparing their citizens for an increasingly competitive economy, they need less burdensome ways of obtaining data to evaluate whether students enrolled in their postsecondary programs are obtaining jobs.

The audit or evaluation exception under FERPA permits certain parties access, without prior written consent, to personally identifiable information from students' education records in order to conduct an audit or evaluation of State or federally supported education programs, or for the enforcement of or compliance with Federal legal requirements relating to those programs.

The proposed amendments would define two terms, "education program" and "authorized representative." These terms are not currently defined in the FERPA statute or its regulations, and the NPRM proposes to define them in the following ways:

- **An education program** would be defined as any program that is 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, regardless of whether the program is administered by an educational authority.

- **An authorized representative** would be defined generally as any entity or individual designated by a State or local educational authority or an agency headed by an official listed in § 99.31(a)(3) – the Secretary, the Comptroller General of the United States, or the Attorney General of the United States – to conduct, with respect to Federal or State supported education programs, any audit, evaluation, or compliance or enforcement activity in connection with Federal legal requirements related to those programs.

The NPRM would also clarify that these officials may receive personally identifiable information from education records to conduct an audit or evaluation of the State or federally funded education programs of either the entity disclosing the personally identifiable information or the entity receiving the personally identifiable information. For example, an SEA may designate a State health and human services agency as its authorized representative in order to conduct an evaluation of one of the SEA's State or federally funded education programs, or one of the health and human services' State or federally funded education programs, such as Head Start. It is vital to ensure that all State or federally funded education programs are adequately preparing children for success in the next stage of life, whether that is in kindergarten or the workforce. It is critical that we assess all taxpayer funded programs so that we target our investments effectively and learn what works and what does not.

In order to increase the accountability of those using personally identifiable information from education records for an audit or evaluation, the NPRM proposes requiring a State or local educational authority or an agency headed by an official listed in § 99.31(a)(3) to use a written agreement that designates any authorized representative to whom it will redisclose personally identifiable information from education records without consent. As we have previously stated in connection with the studies exception, the written agreements should not be entered into lightly or serve only as a pretense to allow the disclosure of personally identifiable student information. The decision for who should be made an authorized representative and what information is necessary to disclose should only be made after thorough deliberation. As proposed in the NPRM, the written agreement must:

1. Designate the individual or entity as an authorized representative;

2. Specify the information to be disclosed and that the purpose for which the information is disclosed to the authorized representative who is to carry out an audit or evaluation of Federal or State supported education programs, or to enforce or comply with Federal legal requirements that relate to those programs;

3. Require the authorized representative to destroy or return to the State or local educational authority or agency headed by an official listed in § 99.31(a)(3) personally identifiable information from education records when the information is no longer needed for the purpose specified and identify the time period in which the information must be returned or destroyed; and

4. Establish policies and procedures consistent with FERPA and other Federal and State confidentiality and privacy provisions to protect personally identifiable information from education records from further disclosure (except back to the disclosing entity) and unauthorized use, including limiting use of personally identifiable information to only authorized representatives with legitimate interests.

The NPRM emphasizes that the State or local educational authority or an agency headed by an official listed in § 99.31(a)(3) is responsible for using ***reasonable methods*** to ensure that any entity designated as its authorized representative complies with FERPA. The NPRM seeks input on how ***reasonable methods*** should be defined. The Department intends to issue guidance on the best practices for written agreements, ***reasonable methods,*** and other related matters.

FERPA's recordkeeping requirements for data disclosures would remain unchanged by the NPRM. The recordkeeping requirements for personally identifiable information disclosed under certain FERPA exceptions includes recording which parties receive personally identifiable information from the education records and their legitimate interests in obtaining the information. The exhaustive list of the recordkeeping requirements is in § 99.32 of the current regulations. For example, if under the audit or evaluation exception an SEA designated the State health and human services agency as an authorized representative to evaluate the academic readiness of Head Start participants in elementary school, the SEA would be the responsible entity under § 99.32(b)(2)(i) for adhering to FERPA's recordation requirements.

Promoting Research on Effectiveness

States need accurate information to make administrative decisions about where resources are needed most and which investments are having the most impact. SEAs must have the ability to enter into agreements with researchers to conduct studies that can be used to improve instruction across districts within their own State. Studies such as these can help States save money by identifying effective practices and targeting limited resources accordingly, while simultaneously increasing the transparency of taxpayer investments.

The studies exception permits non-consensual disclosure of personally identifiable information from education records to an organization that is conducting a study for specified purposes, including a study to be used to inform ways to improve instruction, on behalf of an educational agency or institution. The NPRM proposes to amend the studies exception in the regulations to clarify that a State or local educational authority or an agency headed by an official listed in § 99.31(a)(3) is not prevented by FERPA from entering into agreements with organizations to conduct studies and from redisclosing personally identifiable information from education records on behalf of educational agencies and institutions under §99.33(b) for purposes of conducting studies. Oftentimes school districts do not have the resources available to conduct the studies necessary to improve instruction. For example, an LEA may not have the funds to pay for the study or the staff to interact with the researchers and provide the needed information. Likewise, a study done only at the district level may not be comparable across districts or highlight patterns in similar programs. A study done by an SEA can make better use of limited resources through the consolidation of what would otherwise be individual efforts by districts. An SEA may also wish to conduct a study comparing program outcomes across districts to further assess what programs provide the best instruction and then duplicate those results in other districts.

The NPRM proposes to apply the current requirement for educational agencies and institutions to enter into written agreements with the organizations conducting studies under the studies exception to State and local educational authorities and agencies headed by an official listed in § 99.31(a)(3). The agreements:

1. Must specify the purpose, scope, and duration of the study or studies and the information to be disclosed;

2. Require the organization to use personally identifiable information from education records only to meet the purpose or purposes of the study stated in the written agreement;

3. Require the organization to conduct the study in a manner that does not permit personal identification of parents and students by anyone other than representatives of the organization with legitimate interests; and

4. Require the organization to destroy or return all personally identifiable information when the information is no longer needed for the purposes for which the study was conducted and specifies the time period in which the information must be returned or destroyed.

Parents and students put their trust in the stewards of education data to ensure students' personal information is properly safeguarded and is used only for legitimate purposes and only when absolutely necessary. The Department deeply values this trust and strives to ensure it is doing all it can do to protect the privacy of our students as the uses of their data to improve education increase.

We welcome your feedback on our proposed amendments in the NPRM and encourage the public to comment at: www.regulations.gov ***by the deadline of 5/23/11.***