THE SECRETARY OF EDUCATION
WASHINGTON, DC 20202

January 13, 2014

Honorable Edward J. Markey
United States Senate
Washington, DC 20510

Dear Senator Markey:

Thank you for your letter of October 22, 2013, in which you express concerns regarding the collection and use of sensitive information about students by private parties. I appreciate your concern about the privacy rights of parents and students and, like you, believe that students' personal information should be protected against inappropriate access or use. Indeed, as education data are digitized and the use of these data to improve education has grown, the need to exercise care in the handling of personal information has intensified. Recognizing the need for better guidance and technical assistance in this area, the Department of Education's (Department's) student privacy initiatives have expanded to include the establishment of a Chief Privacy Officer, who leads the Department's Privacy, Information, and Records Management Services division, which is dedicated to advancing the responsible collection, use, and stewardship of information; the creation of the Privacy Technical Assistance Center (PTAC) to provide technical assistance involving privacy; and the issuance of additional guidance on privacy topics (see the enclosed for a listing of examples of these guidance documents).

As you note, the efficient collection, analysis, and storage of student information can help educators find better ways to educate students. When outsourcing school functions, however, schools must ensure that vendors and service providers are properly protecting student information. The Department's obligation is to protect student privacy while providing educational agencies and institutions with the flexibility to outsource institutional services and functions to carry out their educational responsibilities. The Department remains committed to assisting schools and school districts through its administration of the Family Educational Rights and Privacy Act (FERPA) and the Protection of Pupil Rights Amendment (PPRA), including by offering guidance around privacy best practices.

I have enclosed responses to your specific questions. Please do not hesitate to have your staff contact the Department's Office of Legislation and Congressional Affairs at (202) 401-0020 if you have further questions. Again, thank you for your attention to the privacy rights of parents and students.

Sincerely,

/s/

Arne Duncan

Enclosure

Introduction

The Family Educational Rights and Privacy Act (FERPA) requires that educational agencies and institutions (schools and school districts) that receive funds from any program administered by the U.S. Department of Education (Department) provide parents with certain rights relative to students' education records. Certain FERPA provisions also apply to state educational agencies (SEAs), including when they re-disclose education records as part of outsourcing functions. The statute is found at 20 U.S.C. § 1232g, and the regulations are found at 34 CFR Part 99.

FERPA provides parents, with respect to their children's education records, the right to:

- Inspect and review education records within 45 days of a request;
- Seek to amend education records believed to be inaccurate; and
- Consent to the disclosure of personally identifiable information (PII) from education records, except as specified by law.

These rights transfer to the student when he or she turns 18 years of age or enters a postsecondary institution at any age ("eligible student").

The Family Policy Compliance Office (FPCO) in the Department administers FERPA and is responsible for investigating violations of the law and providing school officials with technical assistance and guidance. FPCO also administers the Protection of Pupil Rights Amendment (PPRA), which governs the administration of surveys soliciting specific categories of information, and provides certain requirements concerning the collection and use of student information for marketing purposes. FPCO's Web site is located at: www.ed.gov/fpco.

Under FERPA, a parent or eligible student must provide written consent before an educational agency or institution discloses PII from the student's education records to third parties. There are several statutory exceptions to FERPA's general consent requirement; we discuss below those that may relate to your questions. One exception (referred to below as the "school official exception") generally permits disclosures to "school officials" with legitimate educational interests, including contractors, consultants, volunteers, and other outside parties performing institutional services or functions. Another exception permits an educational agency or institution to disclose education records to "authorized representatives" of state and local educational authorities, the Secretary, the Attorney General of the United States, and the Comptroller General of the United States in connection with an audit or evaluation of federal or state supported education programs, or for the enforcement of or compliance with federal legal requirements which relate to those programs (referred to below as the "audit or evaluation exception"). A third exception allows a school or a school district to disclose "directory information" such as a student's name, address, telephone number, date and place of birth, honors and awards, and dates of attendance. However, a disclosure under this exception is subject to certain requirements, including that the school or school district must first notify parents and eligible students about the types of PII disclosed as "directory information" and must allow parents and eligible students a reasonable amount of time to request that the school or school district not disclose their information.

1. **In 2008 and 2011, the Department issued new regulations with respect to FERPA that addressed how schools can outsource core functions such as scheduling or data management and how third parties may access confidential information about students. These changes also permit other government agencies that are not under the direct control of state educational authorities, such as state health departments, to access student information. Please explain those changes.**

    a. **Why did the Department make these changes?**

    b. **Did the Department perform any analysis regarding the impact of these changes on student privacy? If yes, please provide it. If not, why not?**

In 2008, the Department amended the FERPA regulations regarding the school official exception to clarify that schools and school districts may choose to disclose PII from student education records to contractors, consultants, volunteers, and other outside parties to whom they wish to outsource institutional services or functions that they would otherwise use employees to perform. This amendment to the school official exception is narrowly tailored, in that the outside party must be under the direct control of the school or district with respect to the use and maintenance of the education records, and is subject to the same conditions governing the use and re-disclosure of education records that apply to other school officials under FERPA. Additionally, the arrangement must comply with the criteria specified in the school or district's annual notification of FERPA rights.

The 2008 amendments clarified the circumstances under which schools and school districts could engage volunteers and contract with outside entities to perform needed services or functions on their behalf when sharing PII from education records. For example, many districts outsource the development and/or operation of their information technology systems, such as their student records system. In order for the district's contractor to operate that records system, it would need to have access to student information. As another example, many schools and districts do not have a full-time attorney on staff and outsource legal services to an outside attorney or firm. This amendment clarified that schools and districts have the flexibility to choose to outsource services, provided they comply with the regulations, e.g., by using reasonable methods to ensure that school officials (including contractors, consultants, volunteers, and other outside third parties performing institutional services or functions) obtain access only to education records in which they have legitimate educational interests.

The 2011 FERPA regulatory changes to the audit and evaluation exception clarified how PII from student education records may be disclosed to "authorized representatives" of state and local educational authorities, the Secretary, the Attorney General of the United States, and the Comptroller General of the United States. Our prior interpretations of FERPA on this point had varied over the years, and we felt it necessary to clarify that an authorized representative need not be under the direct control of one of the foregoing authorities in order to receive PII to conduct an audit or evaluation. This is not an expansive interpretation, however, because FERPA permits a school or district to disclose PII to authorized representatives only for the specific limited purposes in the statute, i.e., in connection with an audit or evaluation of federal

or state supported education programs, or for the enforcement of or compliance with federal legal requirements that relate to those programs. To ensure that these authorities put appropriate controls in place when designating an individual or entity as an authorized representative, we added a requirement that there be written agreements between these authorities and the individuals or entities they designate as their authorized representatives if they are not employees, and that these authorities also must use reasonable methods in order to ensure that their authorized representatives comply with FERPA.

In developing the 2008 and 2011 regulations, the Department thoroughly deliberated on the impact that the regulations would have on student privacy and aimed to ensure that any data disclosures are accompanied with appropriate protections and enforcement. In both cases, in responding to comments about the impact of the changes on students' and parents' privacy rights, we carefully considered and responded to the comments and made changes to address commenters' concerns.

2. **Has the Department performed an assessment of the types of information that are shared by schools with third party vendors, including but not limited to contact information, grades, disciplinary data, test scores, curriculum planning, attendance records, academic subjects, course levels, disabilities, family relationships, and reasons for enrollment? If yes, please provide it. If not, why not?**

    a. **Should parents, not schools, have the right to control information about their children even when their data is in the hands of a private company?**

    b. **Do you believe that parents should have the right to choose which information is shared by schools with third party vendors and which is kept confidential? In other words, is it the Department's view that some elements of personal data are more sensitive than others, and therefore deserve greater protections?**

The Department's experience has been that schools routinely share information with outside parties to help provide services and functions that school employees would otherwise perform. This has always been permitted by the FERPA statute, and the 2008 FERPA regulatory amendments were intended to resolve uncertainty about the specific conditions under which schools may disclose PII from education records on their students to contractors, consultants, volunteers, and other outside parties assisting them in performing administrative services and functions.

FERPA allows disclosure without consent because there are essential and legitimate educational needs to disclose data where parental control cannot be reasonably implemented. Obtaining consent is not feasible in some instances, such as when a school district is disclosing PII from education records on its students to a contractor to operate the district's student records system. When a school or school district utilizes one of FERPA's statutory exceptions to disclose information without prior consent, we believe that transparency is critically important, and we recommend to schools and school districts that they be clear – including in their contracts –

about what information is collected about students, how it is used, how it is protected, how and with whom it is shared, and for what specific purpose. Although FERPA does not require this much transparency, we consider it a best practice, and we strongly promote it through technical assistance and guidance.

3. **Has the Department issued federal standards or guidelines that detail what steps schools should take to protect the privacy of student records that are stored and used by private companies? For example, are there guidelines about access to the information, how long it can be retained, how it will be used, whether it will be shared with other parties (including but not limited to colleges to which students apply), and if it can be sold to others? If yes, please provide those standards or guidelines. If not, why not and will the Department undertake the development and issuance of such guidelines?**

The Department is committed to providing guidance to stakeholders on protecting the privacy of student records. A few of the guidance documents we have released include:

- Cloud Computing (June 2012): http://ptac.ed.gov/sites/default/files/cloud-computing.pdf

- Data Security:
  - Identity Authentication Best Practices (July 2012): http://ptac.ed.gov/sites/default/files/authentication.pdf
  - Data Security and Management Training: Best Practice Considerations (Dec. 2011): http://ptac.ed.gov/sites/default/files/issue-brief-security-training.pdf
  - Top Threats to Data Protection (Dec. 2011): http://ptac.ed.gov/sites/default/files/issue-brief-threats-to-your-data.pdf

- Guidance for Reasonable Methods and Written Agreements (Nov. 2011): http://www2.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf

- Data Governance:
  - Data Governance and Stewardship (Dec. 2011): http://ptac.ed.gov/sites/default/files/issue-brief-data-governance-and-stewardship.pdf
  - Data Governance Checklist (Dec. 2011): http://ptac.ed.gov/sites/default/files/data-governance-checklist.pdf
  - Data Stewardship: Managing Personally Identifiable Information in Student Education Records (Nov. 2010): http://nces.ed.gov/pubs2011/2011602.pdf

The Department shares your concerns about commercialization of student data, and intends to provide guidance about how schools and districts can protect student data in connection with contracting for the performance of certain institutional functions or services, such as educational Web services. The guidance will clarify the following key points. When a school or district discloses or re-discloses FERPA-protected data to contract out for certain services, its contractor never "owns" the data, and can only act at the direction of the disclosing entity and in compliance with FERPA. Schools and districts may disclose PII from education records under

the school official exception only if the contractor is performing an institutional service or function for which employees otherwise would be used, and has been determined to have a legitimate educational interest in the education records, as defined by the school or district in its annual notification of FERPA rights. For example, depending on the terms in the agreement, a school or district may require its contractor not only to store education records, but also to develop products for the school or district to use with its students. During the course of providing those services, the contractor could use FERPA-protected information to improve the products the school or district was using. FERPA would permit the school or district to include provisions like this in its written agreement with the contractor. However, FERPA would not allow this contractor to use the FERPA-protected data to create a product never intended for use by the school or district. Similarly, FERPA would not permit a school or district to give FERPA-protected data to a third party solely for it to develop a product to market to a school or district.

The Protection of Pupil Rights Amendment (PPRA) also provides parents with rights with regard to some marketing activities. Specifically, PPRA requires that a school district "directly" notify, such as through U.S. Mail or e-mail, parents of students who are scheduled to participate in specific activities and provide them with an opportunity to opt out of participation in such activities. With limited exceptions, direct notification is required for activities involving the collection, disclosure, or use of personal information collected from students for marketing purposes, or for selling the information or otherwise providing the information to others for marketing purposes. PPRA also requires, with limited exceptions, school districts to develop and adopt policies, in consultation with parents, governing the collection, disclosure, or use of personal information collected from students for marketing purposes. The Family Policy Compliance Office's Web site contains guidance to school superintendents about both FERPA and PPRA. *See* http://www2.ed.gov/policy/gen/guid/fpco/hottopics/index.html.

4. Are there minimization requirements that require private companies to delete information that is not necessary to enhance educational quality for students?

The Department's technical assistance promotes the concept of "data minimization," encouraging educational agencies and institutions to scrutinize the need for PII and to provide de-identified or anonymized data instead, if possible. *See* http://ptac.ed.gov/sites/default/files/case-study5-minimizing-PII-access.pdf. In addition, under FERPA's school official exception to consent, schools and districts must use reasonable methods to ensure that school officials, including contractors, consultants, volunteers, and other outside third parties performing institutional services or functions, only obtain access to those education records in which they have legitimate educational interests. Accordingly, the responsibility is on the school and district not to provide PII from education records to a third party that is not necessary for the performance of the required services. Minimization is a key principle in the Fair Information Practice Principles (FIPPs), and we regularly urge schools and districts to look beyond legal compliance with FERPA and other laws, to focus on FIPPs in making decisions about the use and protection of student data. FIPPs are widely accepted principles that serve as a framework for safeguarding individual privacy in information systems and programs.

Once PII from education records has been disclosed, it is important to ensure that the data are destroyed when no longer needed for the purpose for which they were disclosed. While FERPA does not contain a specific time frame for the destruction of PII that has been disclosed, the exceptions to FERPA's general consent requirement under which PII from education records may be disclosed to conduct studies (20 U.S.C. § 1232g(b)(1)(F)) and to conduct audits and evaluations (20 U.S.C. § 1232g(b)(3) and (b)(5)) do contain specific requirements with respect to the destruction of data. These provisions require that PII from education records be destroyed when no longer needed for the purpose of the study, audit, or evaluation. Furthermore, our regulations also require that there be written agreements for disclosures under these exceptions to organizations conducting studies or to authorized representatives conducting audits or evaluations, and that these written agreements must specify the time period in which the PII from education records must be destroyed. In addition, FERPA's school official exception to consent, under which PII from education records may be disclosed to contractors, consultants, volunteers, and other outside third parties performing institutional services or functions for a school or district, requires that the school or district must maintain direct control over the third party's maintenance and use of education records. This means that a school or district making a disclosure to a third party under the school officials exception is responsible for controlling the length of time that a third party maintains PII from education records.

5. **Do students and their families continue to have the right to access their personal information held by private companies as they would if their personal information were held by educational institutions? If yes, please explain how students and families may exercise this right and how they should be informed of the existence of this right. If not, why not?**

Schools and districts are required to annually notify parents and eligible students of their rights under FERPA. As part of this notification, schools and districts are required to include the procedure for exercising the right to inspect and review education records. Under FERPA, an educational agency or institution, or an SEA, must comply with a request from a parent or eligible student for access to education records within a reasonable period of time, but not more than 45 days after it has received the request. (Some states have laws that require that access to education records be provided to parents and eligible students in shorter periods of time than what FERPA requires.) Accordingly, the school or district is responsible for ensuring parental access, even if the education records are held by a third party contractor. Under the audit and evaluation and studies exceptions, the state or district further disclosing education records is required by FERPA to record the re-disclosures, or to have the school that originally disclosed the education records make such a recordation.

6. **While there are significant potential benefits associated with better collection and analysis of student data, does the Department believe that there also are possible risks when students' personal information is shared with such firms and third parties? If yes, what is the Department doing to mitigate these risks? If not, why not?**

The Department believes that schools and school districts must both protect student privacy and realize the benefits from responsible use of student information. The Department strives to make

this possible through ongoing guidance and technical assistance, as well as through its compliance efforts in FPCO's administration of the law and regulations. In addition to the technical assistance materials listed in our response to question #3, FPCO and the Privacy Technical Assistance Center routinely provide and will continue to provide technical assistance to states, districts, school officials, and parents about student privacy issues, including the sharing of PII with outside parties.

7. **Does the Department require entities that access student data to have security measures in place, including encryption protocols or other measures, to prevent the loss of or acquisition of data that is transferred between schools and third parties? What security measures does the Department require that private companies have in place to safeguard the data once it is stored in their systems?**

FERPA provides that no funds under a program administered by the Department may be made available to any educational agency or institution (school or district) that has a policy or practice of releasing, permitting the release of, or providing access to PII from education records without the prior written consent of a parent or eligible student except in accordance with specified exceptions. In light of these requirements, the Secretary encourages schools and districts to utilize appropriate methods to protect education records, especially in electronic data systems.

Schools and districts are responsible under FERPA for ensuring that they themselves do not have a policy or practice of releasing, permitting the release of, or providing access to PII from education records, except in accordance with FERPA. This includes ensuring that third parties that provide institutional services or functions as ''school officials'' under § 99.31(a)(1)(i)(B) do not maintain, use, or re-disclose education records except as directed by the school or district that disclosed the information. The term ''direct control'' in § 99.31(a)(1)(i)(B)(2) is intended to ensure that a school or district does not disclose education records to a third party unless it can control that party's maintenance, use, and re-disclosure of education records. This could mean, for example, requiring a third party to maintain education records in a particular manner and to make them available to parents upon request.

Exercising direct control could prove more challenging in some situations than in others. Schools and districts outsourcing information technology services, such as Web-based and e-mail services, should make clear in their contracts or service agreements that the third party may not use or allow access to PII from education records, except in accordance with the requirements established by the school or district that discloses the information.

In addition, FERPA's school official exception requires schools and districts to use reasonable methods to ensure that school officials, including contractors, consultants, volunteers, and other outside third parties performing institutional services or functions, only obtain access to those education records in which they have legitimate educational interests. Schools and districts may use physical or technological access controls as reasonable methods. However, irrespective of which access controls are used, schools or districts must ensure that their administrative policies for controlling access to education records are effective and ensure their compliance with FERPA. Our regulations do not require a "one-size-fits-all" approach regarding reasonable

methods for access controls, because we recognize that each school or school district needs to develop its own policies and procedures to meet its individual needs.

If the Department, in performing its investigative responsibilities, found that a school or district was not using reasonable methods of access controls as required under the school official exception, we could find that a violation of FERPA occurred and may take appropriate enforcement action in accordance with FERPA. Additionally, if while investigating a complaint we find that a third party re-disclosed PII from education records it received from a school or district in violation of FERPA, the Department could require the school or district to not allow the third party responsible for the improper re-disclosure access to PII from education records for at least five years.

FERPA's audit and evaluation exception also requires state and local educational authorities, the Secretary, the Attorney General of the United States, and the Comptroller General of the United States to use "reasonable methods" to ensure that any non-employee who accesses or uses PII from education records as an authorized representative complies with FERPA. In the 2011 regulatory changes, the Department amended FERPA to further require a state or local educational authority or an official listed in § 99.31(a)(3), such as the Secretary, to use reasonable methods to ensure "to the greatest extent practicable" that any entity or individual designated as an authorized representative complies with FERPA. Consequently, the Department will consider an entity disclosing PII from education records to its authorized representative without taking reasonable methods to be in violation of FERPA and thus subject to enforcement actions. We issued guidance on the subject of reasonable methods in conjunction with the 2011 rulemaking.
http://www2.ed.gov/policy/gen/guid/fpco/pdf/reasonablemtd_agreement.pdf.

The Department has and will continue to provide guidance and technical assistance that highlight best practices regarding data disclosure, preventing unauthorized disclosure, and data governance. We established a Chief Privacy Officer position and created the Privacy Technical Assistance Center to assist with this sort of guidance.

8. Does the Department monitor whether these third parties are safeguarding students' personal information and abide by FERPA or guidelines released by the Department? If yes, please explain. If not, why not?

As a practical matter, the Department cannot monitor the many thousands of individual contracts between schools and third parties. Rather, we promote best practices and increased understanding of FERPA and PPRA requirements through guidance, technical assistance, and compliance efforts. Our "Guidance on Reasonable Methods and Written Agreements," cited earlier, recommends as a best practice that state and local educational authorities, the Secretary, the Attorney General of the United States, and the Comptroller General of the United States include in their written agreements with their authorized representatives a right to audit or otherwise monitor their authorized representatives. The Department conducts an investigation when we receive a timely complaint providing reasonable cause to believe that there has been a violation of FERPA. Additionally, we have the authority to conduct investigations when we

suspect an educational agency or institution or other recipient of funds under a program administered by the Department has violated FERPA.

The Department has several enforcement measures it can take against recipients of funds under a program administered by the Department. If an educational agency or institution or other recipient of Department funds does not comply during the period of time set under the investigatory process, we may take any legally available enforcement action in accordance with FERPA, including, but not limited to, the following enforcement actions available in accordance with part D of the General Education Provisions Act (20 U.S.C. § 1234c; 34 CFR § 99.66(c)): (1) Withhold further payments under any applicable program; (2) Issue a complaint to compel compliance through a cease and desist order; or (3) Terminate eligibility to receive funding under any applicable program. However, we are required by FERPA to work to bring recipients into compliance before terminating financial assistance (20 U.S.C. § 1232g(f)). As noted previously, in the event that a third party violates FERPA's re-disclosure provisions or does not comply with the destruction requirements under the studies exception, the Department can ban the originating educational agency or institution from disclosing PII to that third party that violated FERPA for at least five years.