Civil Action No. 1:12-cv-00327 (ABJ)

EXHIBIT A

Privacy Technical Assistance Center

For more information, please visit the Privacy Technical Assistance Center: www.ed.gov/ptac

Frequently Asked Questions—Cloud Computing

Overview

The U.S. Department of Education established the Privacy Technical Assistance Center (PTAC) as a "one-stop" resource for education stakeholders to learn about data privacy, confidentiality, and security practices related to student-level longitudinal data systems. PTAC provides timely information and updated guidance on privacy, confidentiality, and security practices through a variety of resources, including training materials and opportunities to receive direct assistance with privacy, security, and confidentiality of longitudinal data systems. More PTAC information is available on www.ed.gov/ptac.

Purpose

This document is designed to assist educational agencies and institutions that are considering using cloud computing solutions for education data. It contains responses to frequently asked questions about meeting necessary data privacy and data security requirements to ensure proper protection of education records. This document addresses compliance with the Family Educational Rights and Privacy Act (FERPA), and, more broadly, provides a short list of additional best practice resources to consider when making decisions about migrating to the cloud.

It is important to keep in mind that FERPA may not be the only statute governing your planned migration to the cloud. In each specific situation, it is necessary to take into consideration any additional applicable federal and individual state data privacy laws that may contain more stringent requirements for data protection than FERPA. PTAC recommends that in evaluating cloud computing alternatives to your current data center solutions you consult with your organization's legal staff to ensure you consider and address all applicable federal, state, and local laws and regulations.

Hosting Education Data on a Commercial Cloud

Question: *Does FERPA allow educational agencies and institutions to use cloud computing solutions?*

Answer: FERPA does not prohibit the use of cloud computing solutions for the purpose of hosting education records; rather, FERPA requires States to use reasonable methods to ensure the security of their information technology (IT) solutions. As noted in the preamble to the December 2, 2011, amendments to the FERPA regulations, "the Federal Government itself is moving towards a model for secure cloud computing. Regardless of whether cloud computing is contemplated, States should take care that their security plans adequately protect student data, including PII [personally identifiable

information] from education records, regardless of where the data are hosted"(Family Educational Rights and Privacy, Final Rule, 76 Federal Register 75612 [December 2, 2011]).

Question: *Does FERPA permit educational agencies or institutions to outsource their information technology IT functions?*

Answer: With regard to the question of whether FERPA permits an educational agency, such as a local educational agency (LEA), or an educational institution, such as an elementary or secondary school, to store education records in a cloud platform environment, FERPA permits an LEA or a school to disclose, without prior written consent, personally identifiable information (PII) from education records to a contractor, consultant, volunteer, or other party to which the LEA or school has outsourced institutional services or functions if the LEA or school meets certain conditions. The Department commonly refers to this exception to the requirement of consent in FERPA as the "school official" exception. The "school official" exception is contained at 34 Code of Federal Regulations (CFR) §99.31(a)(1) of the FERPA regulations (www.ed.gov/policy/gen/reg/ferpa/) and sets forth the three conditions that the LEA or school must meet to outsource institutional functions. Specifically, the outside party must: 1) perform an institutional service for which the LEA or school would otherwise use employees; 2) be under the direct control of the LEA or school with respect to the use and maintenance of education records; and 3) be subject to requirements in §99.33(a) of the FERPA regulations governing the use and redisclosure of PII from education records.

The Department made this change to the FERPA regulations in 2008. The preamble to the December 9, 2008, amendments explains the requirement that the LEA or school must maintain "direct control" with respect to the use and maintenance of PII from education records: "Exercising direct control could prove more challenging in some situations than in others. Schools outsourcing information technology services, such as web-based and e-mail services, should make clear in their service agreements or contracts that the outside party may not use or allow access to personally identifiable information from education records, except in accordance with the requirements established by the educational agency or institution that discloses the information" (Family Educational Rights and Privacy, Final Rule. 73 Federal Register 74816 [December 9, 2008]).

When the entity desiring to outsource its IT functions is a State educational agency (SEA), rather than an LEA or a school, the school official exception does not apply. SEAs may rely on the audit or evaluation exception at 34 CFR §§99.31(a)(3) and 99.35 of the FERPA regulations to outsource IT functions. While outsourcing IT functions would not traditionally be considered an audit or evaluation, the Department recognizes that the size and scope of state longitudinal data systems may necessitate outsourcing IT functions, and believes that the use of this exception is appropriate in this instance. Under the audit or evaluation exception, an SEA may disclose education records without consent to a party under its direct control, such as a contractor, who has been designated as the agency's "authorized representative." As described in the December 9, 2008, preamble to the FERPA Final Rule (73 Federal Register 74825), the Department interprets the term "authorized representative" in the audit or evaluation exception to mean contractors, consultants, volunteers, and other outside parties (i.e., nonemployees) that a State educational authority may use to perform institutional services for which it would otherwise use its own

employees. For example, an SEA may disclose PII from education records, without consent, to an outside computer consultant hired to develop and manage a data system for education records. (Note that disclosures made under the audit or evaluation exception after the January 3, 2012, effective date of the new FERPA regulations require that an SEA must use a written agreement that complies with 34 CFR § 99.35[a][3] to designate any authorized representative other than an employee of the SEA, unless the SEA had a written agreement in place with the authorized representative prior to January 3, 2012. In that case, the SEA must put in place a written agreement that complies with 34 CFR § 99.35[a][3] only upon the renewal of or amendment to the written agreement that predates January 3, 2012.)

Question: *Are there recommended best practices to help agencies decide whether they should move to the cloud? Can the Department recommend which cloud solution to use?*

Answer: The Department cannot recommend any specific cloud solution over another. Deciding which solution is the best for your organization should be made on a case-by-case basis, after conducting a careful risk management assessment. Some security questions to consider include, but are not limited to:

1. Does the cloud solution offer equal or greater data security capabilities than those provided by your organization's data center? To determine this, you should review and compare available solutions, including firewalls, patch management procedures, security monitoring and response methods, and other relevant data security measures.

2. Have you taken into account the vulnerabilities of the cloud solution? You should consider that cloud services are an increasingly attractive target for hackers. Some clouds have experienced direct malicious attacks, potentially exposing any information stored there. In other instances, the clouds have been the targets of denial of service attacks.

3. Have you considered that incident detection and response can be more complicated in a cloud-based environment? You should evaluate your existing incident response capabilities and determine if changes are needed before deciding whether to move to the cloud. Organizational policies and procedures may need to be updated to accommodate anticipated changes introduced by the addition of a cloud-based system. Any such changes should be made well in advance of the implementation and updated regularly.

4. Have you considered that metrics collection, and system performance and security monitoring are more difficult in the cloud? You should define what metrics you need to collect and determine the desired level of security monitoring as part of the planning process of a potential move to the cloud.

In addition to security considerations, there are many other factors to keep in mind when deciding whether to move your data to the cloud. Potential concerns span a range of domains, including privacy, legal, and compliance issues. Several specific questions to consider include:

1. How will your agency exercise control over the data within the cloud to ensure that the data are available and that confidentiality and integrity of the data remain protected? Are there appropriate access and use controls in place to provide proper level of accountability? Are there any concerns regarding screening and monitoring of contractor staff and their activities?

2. Have you evaluated potential legal concerns associated with outsourcing data management to a cloud provider? Legal considerations may include ensuring proper protection of intellectual property and various contractual issues, such as end of service matters. For example, your organization must have a way to get the data back in a secure and timely manner in case a cloud provider goes out of business.

3. Have you considered what measures you will need to implement to ensure that the cloud provider complies with all applicable federal, state, and local privacy laws, including FERPA? For example, have you made sure that storing data on the cloud does not interfere with your ability to provide parents and eligible students with access to their education records, should they choose to exercise their FERPA right to inspect and review them? Other considerations related to compliance with FERPA include ensuring that the cloud provider follows proper data use, redisclosure, and destruction procedures, specified at 34 CFR §§99.33(a) and 99.35(b).

You should evaluate existing protection capabilities that your organization and its partners use to secure organizational systems and applications before deciding whether to migrate to a cloud-based solution. Such an evaluation will help to establish a baseline level of protection with which to evaluate potential benefits and risks associated with moving to a cloud-based alternative. While FERPA does not directly address the viability of specific cloud solutions, the Department recognizes that their use is a growing trend and is beginning to pilot its own cloud computing solutions.

Question: *For educational agencies that have already selected a preferred cloud solution, are there recommended best practices when moving to the cloud?*

Answer: The Department is aware that some educational agencies are beginning to deal with this issue and is considering releasing best practice recommendations addressing this topic more in-depth. As a general suggestion, educational agencies are encouraged to focus on ensuring continuing protection of the privacy and security of students' records and minimizing the risk of unauthorized disclosure of the data by developing a cloud computing migration strategy that addresses the organization's specific privacy and security needs. This strategy involves carefully evaluating existing privacy, security, and compliance requirements and establishing expectations of prospective cloud service providers in terms of necessary levels of service and security before engaging with them.

Agencies should carefully consider how moving to a cloud solution will affect their existing privacy and security controls. Transitioning to the cloud may present an opportunity for improving the effectiveness and efficiency of existing procedures as an agency is making the changes necessary to implement and

manage a cloud-based solution. Moving data into the cloud can also significantly change the agency's legal requirements for the protection and handling of data. It is important to consult with your organization's legal counsel to fully understand the ramifications of implementing a cloud solution and the effect it may have on your organization's operations. Please see a list of resources at the end of this document for additional best practices information.

Keeping Education Records Stored Within the United States

Question: *Does FERPA require that confidential information in the cloud be stored within the United States? Is there a best practice?*

Answer: The preamble to the December 2, 2011, amendments to the FERPA regulations states the following in response to a comment on this general subject:

"FERPA makes no distinctions based on State or international lines. However, transfers of PII from education records across international boundaries, in particular, can raise legal concerns about the Department's ability to enforce FERPA requirements against parties in foreign countries. It is important to keep in mind that for a data disclosure to be made without prior written consent under FERPA, the disclosure must meet all of the requirements under the exceptions to FERPA's general consent requirement. For example, if the conditions under the audit or evaluation exception in FERPA are met, a State educational authority could designate an entity in a different State as an authorized representative for the purpose of conducting an audit or evaluation of the Federal- or State-supported education programs in either State. The disclosure of PII from education records is not restricted by geographic boundaries. However, disclosure of PII from education records for an audit or evaluation of a Federal- or State-supported education program is permitted only under the written agreement requirements in § 99.35(a)(3) that apply to that exception. Under these requirements, the disclosing entity would need to take reasonable methods to ensure to the greatest extent practicable that its authorized representative is in compliance with FERPA, as is explained further under the *Reasonable Methods (§ 99.35(a)(2))* section in this preamble. More specifically, an LEA could designate a university in another State as an authorized representative in order to disclose, without consent, PII from education records on its former students to the university. The university then may disclose, without consent, transcript data on these former students to the LEA to permit the LEA to evaluate how effectively the LEA prepared its students for success in postsecondary education" (Family Educational Rights and Privacy, Final Rule. 76 Federal Register 75611-75612 [December 2, 2011]).

While FERPA does not explicitly require that education data be stored within the U.S., it does hold the disclosing entity legally accountable for protecting the confidentiality of PII from education records. This includes compliance with the "direct control" requirement that applies to schools and LEAs disclosing PII from education records under the "school official" exception, and the requirement for written agreements and the use of reasonable methods to ensure that the information is adequately protected that applies to SEAs disclosing PII from education records to their authorized representatives under the

"audit or evaluation" exception. Regardless of which exception is used, it is important to be aware that it is often difficult to take enforcement actions against entities outside of the U.S. under U.S. privacy laws and regulations, and to hold these entities legally accountable for violations of contracts or written agreements. Therefore, storing sensitive education records, including medical, behavioral, assessment, and related information in special education case files, within the U.S. would be considered a best practice as it ensures that they are subject to U.S. jurisdiction.

Additional Resources

The resources below include links to federal regulations and several guidance documents outlining security issues and threats to consider before migrating applications or services to a cloud environment. Please note that some of the guides come from the private sector (marked below) and, as such, they do not address the legal requirements, including FERPA, that need to be met when warehousing education records. The U.S. Department of Education does not provide endorsement for private-sector resources; it simply refers them to readers for consideration. Additionally, a reference to the Federal Risk and Authorization Management Program guidelines used by federal agencies around cloud computing is provided; these guidelines also do not specifically address the requirements of FERPA-protected data.

- 10 Cloud Computing Security Tips for Small Businesses (private sector resource): www.smallbusinesscomputing.com/biztools/article.php/3927376/10-Cloud-Computing-Security- Tips-for-Small-Businesses.htm
- Cloud Security Alliance, Top Threats to Cloud Computing V1.0 (private sector resource): www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf
- Creating Effective Cloud Computing Contracts for the Federal Government: Best Practices for Acquiring IT as a Service: http://www.cio.gov/cloudbestpractices.pdf
- Federal Risk and Authorization Management Program: www.fedramp.gov
- FERPA regulations amendment released December 9, 2008: www.ed.gov/legislation/FedRegister/finrule/2008-4/120908a.pdf
- FERPA regulations amendment released December 2, 2011: www.gpo.gov/fdsys/pkg/FR-2011-12-02/pdf/2011-30683.pdf
- National Institute of Standards and Technology, Cloud Computing Guidelines for Managing Security and Privacy: www.nist.gov/itl/csd/cloud-012412.cfm
- National Institute of Standards and Technology (NIST), NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing: www.nist.gov/manuscript-publication-search.cfm?pub_id=909494
- Privacy Technical Assistance Center: www.ed.gov/ptac

Glossary

Authorized representative means any entity or individual designated by a State or local educational authority or an agency headed by an official listed in 34 CFR §99.31(a)(3) to conduct—with respect to Federal- or State-supported education programs—any audit or evaluation, or any compliance or enforcement activity in connection with Federal legal requirements that relate to these programs, 34 CFR §99.3.

Education program means any program 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, and any program that is administered by an educational agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR §99.3.

Education records means records that are directly related to a student and are maintained by an educational agency or institution or by a party acting for the agency or institution. For more information, see the Family Educational Rights and Privacy Act regulations, 34 CFR §99.3.

Personally identifiable information (PII) from education records includes information, such as a student's name or identification number, that can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information. See Family Educational Rights and Privacy Act regulations, 34 CFR §99.3, for a complete definition of PII specific to education records and for examples of other data elements that are defined to constitute PII.