Hogan Lovells

**MEMORANDUM**

Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

**TO** School District Clients and Friends

**FROM** Maree Sneed
Stephanie Gold
Harriet Pearson
Christopher Wolf
Bret Cohen
Michelle Tellock

**DATE** March 12, 2014

**SUBJECT** ***It's 10pm: Do you know who can see (and use, and share…) your students' data?*** **– Department of Education releases new guidance on student data outsourcing**

---

The Department of Education recently ramped up the pressure on school districts and schools to reform their procedures for student data outsourcing, releasing a fourteen-page guidance document on February 25 that reinforces the obligation to comply with privacy laws when using a vendor to host or process student data. By issuing the guidance, the Department has put school districts and schools on notice of its expectations regarding their responsibilities when entering into these arrangements. School districts and schools should therefore carefully consider the guidance and how it affects their student privacy compliance obligations.

The guidance is the latest in a series of events that has shone a spotlight on school district and school use of data processing vendors. Back in October, a Colorado superintendent made the New York Times when she faced stiff opposition from parents and school board members to the district's retention of an online records management vendor that would have resulted in a shift of student records to the vendor's servers. The next month, after the election of a new school board opposed to the use of the vendor, the superintendent announced her retirement – and on the same night, the board voted to scrap the long-debated vendor relationship.

A few weeks after the Times article, Sen. Ed Markey (D-Mass.) sent a letter to the Department requesting information about how student privacy laws, including the Family Educational Rights and Privacy Act ("FERPA"), permit "schools to share student data, without notifying parents, with companies to which they have outsourced core functions like scheduling or data management." On January 13, the Department responded, clarifying that it does not

permit school districts or schools to indiscriminately disclose data to third parties and provides parents and students with important rights when data are held by a vendor.

And in December, the Fordham Center on Law and Information Policy released a report titled "Privacy and Cloud Computing in Public Schools." The report found even though 95% of public school districts rely on online service providers for data processing, those districts frequently surrender control of student information, with fewer than 25% of the agreements specifying the purposes for which the vendor could use the student information and fewer than 7% restricting the sale or marketing of student information. The report concluded that school districts are not dedicating sufficient resources to comply with their privacy obligations with respect to the student data they disclose to third parties, particularly when contracting.

Given this recent scrutiny, school districts and schools should examine whether their data outsourcing practices conform to the legal requirements and best practices described in the Department's guidance, which we summarize in this client alert.

*Scope of the guidance*

The guidance addresses privacy and security considerations when school districts or schools use third-party "online educational services"; that is, computer software, mobile applications, and web-based tools provided by a third party to a school or school district that students and/or parents access via the Internet and use as part of a school activity. Examples of these services include tools that allow students to access course materials, comment on class activities, or complete homework online. The guidance does not address social media or other online services that students may use in their personal capacity, nor does it address school administrators' use of online services to which students and/or parents do not have access, for example, an online student information system for tracking attendance used exclusively by teachers and staff.

*When must schools comply with FERPA when students are online?*

FERPA protects against unauthorized disclosure of personally identifiable information ("PII") from students' education records. With several exceptions, a school may not disclose PII to a third-party provider unless the school has first obtained written permission from parents or eligible students to do so.

The guidance advises that school districts must evaluate the use of online educational services "on a case-by-case basis" to determine whether FERPA-protected information is being used and whether an exception to the consent-to-disclose requirement applies. For example, an online system that requires a school district or school to provide students' names and contact information from education records in order for students and parents to log in and access course material would implicate FERPA. In addition, information about student use of online services that is stripped of student identifiers—such as how long a student took to perform an online task, the date and time the student completed an activity, how many attempts the student made, and

how long the student's mouse hovered over an item—is not protected under FERPA and can be used by a vendor unless the agreement with the school district or school forbids such use.

Notwithstanding the general rule, the FERPA "school official" exception permits under certain circumstances the disclosure of PII to third-party providers without first obtaining written permission. To qualify, the provider must, among other things, (1) perform an institutional service or function for which the school or school district would otherwise use its own employees, (2) be under the "direct control" of the school or school district with regard to the use and maintenance of education records, and (3) use education records only for authorized purposes and not re-disclose PII from education records to other parties without authorization.

Practically, to qualify for the exception a school district or school should enter into a contract that restricts the vendor from using student PII for unauthorized purposes and provides the school district or school with the ability to direct the vendor to use, transfer, or delete student records only at the instruction of the school district or school. In some instances, online educational services require school districts or schools to consent to an online Terms of Service as a condition of using the service. Those Terms are binding contracts, and if they do not comply with FERPA or enable the school district or school to make use of the school official exception, it may violate FERPA to disclose education records to those services.

The guidance also reminds schools that whenever a third-party provider maintains a student's education records, the school must be able to provide parents and eligible students with access to those records. As a result, any agreement with a provider should allow for such access within a reasonable period of time, but not more than 45 days after receiving a request.

*How can providers use student information they collect and receive?*

If a school has shared PII with a provider under the "school official" exception, the provider must use the PII only for the purposes for which it was disclosed. For example, the provider may not (1) use the information to market new products or services, (2) use the information to target students with directed advertisements, or (3) sell the information to a third party. However, if student information has been properly de-identified, or if information has been shared under the FERPA "directory information" exception, which permits disclosure of information that would not generally be considered harmful (e.g., student name and address), such information is not protected by FERPA and is not subject to limitations on use or redisclosure.

On top of FERPA, the Protection of Pupil Rights Amendment ("PPRA") requires school districts and schools, with certain exceptions, to notify parents if students are scheduled to participate in activities that involve the collection, disclosure, or use of student PII for marketing purposes, and gives parents the opportunity to opt out of such activities. To the extent that an online education service plans to make use of student PII for marketing purposes, school districts and schools should work with the service to provide the required notice and effectuate the parental opt-out.

*Best practices for schools*

In the guidance, the Department of Education recommends certain best practices that school districts and schools should consider adopting when contracting with service providers in order to meet their privacy obligations. While not mandatory, the adoption of these best practices can serve as evidence that a school district or school is taking reasonable steps to comply with its FERPA and PPRA obligations in the event of a Department of Education investigation.

- Conduct an inventory of the online educational services being used. This will aid in assessing the information being collected and shared with providers and to evaluate which services are most effective.

- Establish policies and procedures to evaluate and approve vendors prior to implementation. School districts and schools should make clear to teachers and administrators how use of services may be approved and who has the power to approve their use. In particular, school districts and schools should remind teachers and administrators that clicking to accept a Terms of Service serves to enter the school into a contractual relationship, and such Terms of Service must comply with the school district's or school's FERPA and PPRA obligations. The Department also recommends that established approval procedures be followed when deciding to use free online educational services, including the review of their Terms of Service, to ensure that they do not present a risk to privacy or security of students' data or to the school's IT systems.

- Use a written contract or legal agreement, when possible, to maintain required "direct control" over the use and maintenance of student data. The Department recommends that agreements include provisions that (1) address data ownership, responsibilities in the event of a data breach, and minimum security controls; (2) specify the information the provider will collect; (3) define the specific purposes for which the provider may use student information and bind the provider to only those approved uses; (4) specify whether the school, parents, and eligible students will be permitted to access the data and explain the process for obtaining access; (5) establish procedures for modifying and terminating the agreement, and specify how student information will be disposed of upon termination; and (6) clarify the parties' responsibilities to indemnify one another and what the provider must do to remedy a violation of applicable state and federal laws, including FERPA and PPRA, or to compensate the school for such a violation.

- Employ extra caution when using "click-wrap" consumer applications that do not allow users to negotiate agreements before using the application. The Department recommends that school districts and schools review an online service's Terms of Service at the time of sign-up and regularly thereafter to determine if any provisions have changed. Schools and school districts should also save a copy of the Terms of Service to which they agreed and limit teachers' ability to accept Terms of Service without going through appropriate approval channels.

- Be transparent with parents and students about how the school collects, shares, protects, and uses student data. Schools and school districts must provide parents and eligible students with specific notices under FERPA and PPRA, but the Department also recommends that schools and school districts develop a plan that addresses student privacy and information security issues in order to alleviate confusion about how data will be shared and how they will be used.

- Consider on a case-by-case basis whether obtaining parent consent may be appropriate. The Department recommends this as a best practice even when FERPA does not require consent.

Conclusion

Schools and school districts are encouraged to remember their important role in setting policies to protect student privacy and to consider carefully the appropriate uses of online educational services. We hope this information is useful to you as you consider your schools' policies and practices related to online educational services.

* * *

If you have questions about the guidance or applicable regulations more generally, please contact Maree Sneed at 202-637-6416 or maree.sneed@hoganlovells.com or Stephanie Gold at 202-647-5496 or stephanie.gold@hoganlovells.com. In addition, we will be discussing the guidance and its implications for schools and school districts on a webinar hosted by the American Association of School Administrators (AASA) on April 1, 2014 at 1:00pm EDT. Information about the webinar will be available on the AASA website, or please feel free to reach out to us for details.