DATA PRIVACY LAW UPDATE:
TEN THINGS TO ADVISE YOUR SCHOOL BOARD CLIENTS – BEFORE IT’S TOO LATE

- David Rubin, David B. Rubin PC, Metuchen, NJ
- Phil Hartley, Hartley & Hawkins, Gainesville, GA
- Sonja Trainor, NSBA
  Council of School Attomeys, Alexandria, VA
“Cloud services are poorly understood, non-transparent, and weakly governed: only 25% of districts inform parents of their use of cloud services, 20% of districts fail to have policies governing the use of online services, and a sizeable plurality of districts have rampant gaps in their contract documentation, including missing privacy policies.”

PRIVACY AND CLOUD COMPUTING IN PUBLIC SCHOOLS, FORDHAM, DECEMBER 2013

http://www.fordham.edu/info/23830/research/5917/privacy_and_cloud_computing_in_public_schools
School Official Exception – PII may be disclosed without consent to...

1. other school officials, ... whom the agency or institution has determined to have legitimate educational interests.

2. A contractor, consultant, volunteer, or other party to whom an agency or institution has outsourced institutional services or functions may be considered a school official under this paragraph provided that the outside party—

   (1) Performs an institutional service or function for which the agency or institution would otherwise use employees;

   (2) Is under the direct control of the agency or institution with respect to the use and maintenance of education records; and

   (3) Is subject to the requirements of § 99.33(a) governing the use and redisclosure of personally identifiable information from education records.

   (ii) An educational agency or institution must use reasonable methods to ensure that school officials obtain access to only those education records in which they have legitimate educational interests. An educational agency or institution that does not use physical or technological access controls must ensure that its administrative policy for controlling access to education records is effective and that it remains in compliance with the legitimate educational interest requirement in paragraph (a)(1)(i)(A) of this section.

"DIRECT CONTROL" 34 C.F.R. 99.31

1. THINK IN TERMS OF “DATA,” NOT RECORDS
E-mail
District-based servers
Cloud storage
Classroom apps
Online IEPs
Text messages
Metadata

2. KNOW WHERE YOUR STUDENT DATA IS GOING AND UNDER WHAT AUTHORITY
QUESTIONS TO ASK

- How is access to student data managed and controlled within the District?
- Where does student data get sent outside of the District and who does it?
- What statute or legal authority allows it to be sent?
- Does there exist a procedure or a contract that controls what is sent and how?
- Has the contract or procedure been reviewed for legal issues?

PROACTIVE MEASURES

- Initiate or update a data audit or inventory that includes answering these questions
- Make sure that the District’s procurement, technology and curriculum selection policies or procedures include all contracts with technology vendors and that everyone in the District has been trained to insure that those are followed
- Make sure that the District and its vendors understand what it means when a vendor is designated as a “school official” under FERPA for purposes of sharing PII
- Make sure that all those involved in the process know enough about federal and state law to understand the risks and insure compliance, especially important to coordinate between legal and technology functions and review
3. MAKE NECESSARY ADJUSTMENTS NOW TO INCREASE SECURITY AND ACCESSIBILITY OF DATA.
Clearly worded acceptable use policy
Assigning specific job responsibility
Eliminating opportunities for security breaches
Inventory/Network Mapping
Authentication protocols/Strong Passwords
“Defense in Depth” architecture

4. BE TRANSPARENT ABOUT DATA SHARING, MAINTENANCE, DISCLOSURE, AND UNDER WHAT CONDITIONS IT’S DESTROYED.
U.S. DEPT. OF ED. PRIVACY TECHNICAL ASSISTANCE CENTER RECOMMENDS

“[T]he Department recommends that schools and districts clearly explain on their Websites how and with whom they share student data, and that they post any school and district policies on outsourcing of school functions, including online educational services. Schools and districts may also want to post copies of the privacy and security provisions of important third party contracts.”

http://ptac.ed.gov/

- Existing state laws on open records and records retention and new state laws on student data privacy
- Existing FERPA and PPRA notice requirements to parents (and in some cases state laws as well)
- Does the policy match the website match the handbook match the contract? Know which controls what issue and what the purpose of each is.
- Don’t make promises in the name of transparency that you can’t keep technologically or that cost a lot - consult the tech folks before drafting all of these notices

WHAT DO YOU SHARE WHERE AND COORDINATED WITH WHAT?
5. KNOW YOUR STATE REQUIREMENTS FOR PARENT OPT-OUT/IN OF DATA DISCLOSURE, AND HAVE CLEAR POLICIES.

- What Does Federal Law Require?
  - FERPA
  - PPRA
  - COPPA
- What Does Your State Law Require?
  - Notice of additional rights
  - Notice of opt-in/opt-out
- Be careful that local policies and procedures do not create additional rights
  - Effect on instruction
  - Effect on administration
6. ADOPT CLEAR AND WELL-COMMUNICATED POLICIES AND PROCEDURES REGARDING PURCHASING AND USING HARDWARE, SOFTWARE, AND ONLINE EDUCATION TOOLS (APPS).

Decentralized Review
- Teachers have more freedom to review apps prior to use
- District must provide detailed guidance/checklist to address instructional, privacy and security concerns

Centralized Review
- District has list of pre-approved online apps for use in classroom, and/or strong contract addenda
- All staff authorized to negotiated contracts must do so consistently, using the same form agreements
- Recommended by FCC with respect to school district consent for student use of websites aimed at students under 13.
Massachusetts Student Privacy Alliance (MSPA)
Student Data Privacy Consortium formed under Access 4 Learning (A4L) Community

SCHOOL DISTRICT CONSORTIA – COMMON STUDENT DATA CONTRACTS AND ADDENDA

Common Sense Media’s Graphite program
https://privacy.graphite.org

U.S. ED’s Privacy Technical Assistance Center’s guidelines for reviewing terms of service (2014) and model terms of service

TOOLS FOR REVIEWING APP PRIVACY TERMS
7. LIMIT VENDOR USE OF STUDENT DATA ACCORDING TO WIDELY-ACCEPTED PARAMETERS.

Student data privacy principles are now more widely accepted.
COMMON PRIVACY PROVISIONS

- Student records are **property** of and under the **control** of the school district;
- How **students** may **retain possession and control** of their own content;
- No third party **use** of any student information for any purpose other than those required or specifically permitted by the contract;
- Procedures by which a parent or eligible student may **review PII and correct** erroneous information;
- Actions third party will take to ensure the **security and confidentiality** of student records;
- Procedures for **notifying** the affected parent or eligible student in the event of an unauthorized **disclosure**;
- Student’s records shall not be retained or available to the third party upon **completion of the contract** how enforced
- How the district and the third party will jointly ensure **compliance with FERPA**; and
- Third party may not use PII to engage in **targeted advertising**.

8. **Implement ongoing staff training on data privacy concerns, procedures, policies and parent questions.**
- Low-to-no cost Apps
- No Supervisory oversight
- No centralized procurement
- New legislation assumes staff awareness
- Effective staff training is essential
9. INSTALL A DEDICATED CHIEF PRIVACY OFFICER, DATA GOVERNANCE COMMITTEE OR OFFICE WITHIN EACH DISTRICT.

- Data Governance Program: overall management of organization’s data
- Outline policy, standard procedures, responsibilities, and controls at every point in the data life cycle:
  - Define
  - Collect
  - Store and Protect
  - Use
  - Share
  - Retire

- Data Governance group or Chief Privacy Officers answer questions, create policy, enforce policy:

National Forum on Education Statistics Guide to Education Data Privacy

SELECT THE PERSON/GROUP IN CHARGE
Encouraged by Fed:
- Data Sharing Toolkit for Communities (March 2016)
  - FERPA may allow data-sharing, especially when student information is de-identified and aggregated, to provide wrap-around services to students

10. BE READY FOR CHANGES TO FERPA, INCLUDING AN INCREASED ENFORCEMENT ROLE FOR THE U.S. DEPARTMENT OF EDUCATION.
“Federal law must be strong enough to protect student information in an increasingly digital school environment yet broad enough to allow states and districts to innovate.”

ED and FTC should provide clarity on how FERPA/PPRA work together with COPPA.

Fed should support states and districts through funding, training, and technical assistance (expand capacity to protect student information)

--Data Quality Campaign, NASBE

WHAT’S THE FEDERAL ROLE?

Definitions update (“maintained electronically or physically”)

Additional security and privacy policies

Prohibition on marketing/advertising (restrictions on vendor handling)

Transparency - LEA must notify parents of security/privacy policies and actions, contracts with vendors, including posting online

FERPA BILLS - KEY PROVISIONS
FERPA BILLS – KEY PROVISIONS

- Enforcement authority of ED
  - New office to monitor compliance, investigate, process, review and adjudicate violations and complaints
  - Fines against school districts - $2000 per student harmed to a max of $500,000
  - Refer ed service provider violators to FTC
- Designated school official with responsibility for security (privacy?) of district data
- Parent access, procedural protections strengthened and flow through to data held by ed service provider

FERPA BILLS - KEY PROVISIONS

- Limits on research studies exception
- Response time for parent request for records shortened (from 45 to 30 days)
- Breach notification required within 3 days
- LEA can only release student ed records/ PII/ data to ed service provider that has met certain requirements, and only pursuant to written agreement with certain specs, including acceptable uses of PII.
ESSA still requires data collection, and in fact adds 3 categories about which LEA and State must report information on student achievement:
- Students in foster care
- Homeless students
- Students with parents in the Armed Forces

ESSA allows Title II PD grants to be used for activities including data literacy and data privacy training.

Civil Rights Data Collection
White House issued reports on Big Data in May 2014 and 2016.

Proposed rule on disproportionality in special education depends on data collection.

DATA IS ON WASHINGTON’S RADAR

NSBA Guide for school board members
http://www.nsba.org/data-cloud

COSA Guide for school attorneys

Seminar paper: Negotiating Contracts for Cloud Computing by Tokarz, October, 2015

Kappan article on Student Data Privacy February 2015:
http://pdkintl.org/noindex/k_v96/13pdk_96_5.pdf

NSBA/COSA RESOURCES
NASBE RESOURCES

- NASBE publication The Standard, May 2016: The Power of Data
  http://www.nasbe.org/standard-issue/the-power-of-data/
- NASBE - DQC webinar May 26, 2016: State Legislative Recap
- NASBE article April, 2016: A Tale of Two Federal Student Data Privacy Bills
  http://www.nasbe.org/project/education-data-privacy/nasbe-resources/

NASBE RESOURCES

- Checklist for Developing School District Privacy Programs
- Responsibilities of Third-Party Service Providers under FERPA
- Contractor Responsibilities under the FERPA’s Audit or Evaluation Exception
- Policies for Users of Student Data Checklist
- Protecting Student Privacy While Using Online Educational Services - Model Terms of Service
- Protecting Student Privacy While Using Online Educational Services
- Transparency Best Practices
- Best Practices for Data Destruction
- Data Breach Response Training Kit

http://ptac.ed.gov/
Data Sharing Toolkit for Communities (March 2016)

FERPA for School Officials

PPRA FAQ, Model Notices

MORE RESOURCES

Data Quality Campaign - Student Privacy Legislation 2015+
http://dataqualitycampaign.org/resources/

Future of Privacy Forum - Data De-Identification+
https://fpf.org/

Consortium for School Networking -- Protecting Privacy Toolkit+
http://www.cosn.org/focus-areas/leadership-vision/protecting-privacy

White House Big Data Reports
  https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf
  https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

MORE RESOURCES
THANK YOU!