Student Data Breaches: Is Your District Prepared?

Colleen A. Sloan, Esq., Manager, Labor Relations and Associate School Attorney
JoAnn Balazs, Director, Management Services
Janell Hallgren, Manager, Policy Services

Data Security Symposium - July 25, 2013
Summary of today’s session:

• Unauthorized disclosure of student data can occur, despite best efforts

• In this session, we will:
  – Review legal obligations under FERPA and NYS Technology Law to notify affected parties in the event of a breach of student data
  – Review suggested policies and administrative regulations to assist your district in implementing “best practices” in data breach prevention, response and notification
• Chapters 442 and 491 of Laws of 2005

• Added NYS Technology Law §208:
  – Requires “state entities” to notify persons of an unauthorized acquisition of their private information resulting from a breach of information security
  – Cities, counties, municipalities, villages, towns, and other local agencies are exempted from definition of “state entity”
  – School districts/BOCES are “local agencies” for purposes of this law

• BUT must adopt a notification policy or pass a local law consistent with the requirements of Section 208
What is “Private Information”? 

(1) 

An individual’s “personal information” … 

any information concerning a natural person which, because of name, number, symbol, mark or other identifier, can be used to identify that natural person
What is “Private Information”? 

(2) ... in combination with one or more of the following data elements.....

– Social Security Number, or

– Driver’s License Number or Non-Driver ID, or

– Account number, credit or debit card number AND the security code, access code or password which permits access to an individual’s financial account
What is “Private Information”?

(3) ...

... when either the personal information or the data element is not encrypted (or encrypted with an encryption key that has also been acquired)

All 3 elements must be present
What is a Security Breach?

• Under STL §208:

  “An unauthorized acquisition of computerized data which compromises the security, confidentiality or integrity of personal information maintained by the entity”

  “Good faith” acquisition by an employee for agency-related purpose is not a breach
Under STL § 208, must notify:

- “Owned or licensed” computerized data:
  - Any NYS resident whose private information was acquired

- “Maintained” computerized data:
  - Owner or licensee of the information

- Whenever NYS residents notified, also notify:
  - New York State Attorney General's Office
  - New York State Office of Cyber Security
  - New York State Department of State Division of Consumer Protection

- If more than 5,000 NYS residents notified, also notify:
  - Consumer reporting agencies
Methods of Notification

• Written
• Electronic
• Telephone

• Substitute notice, under certain circumstances
  – E-mail
  – Conspicuous posting on website
  – Notification to statewide media
In February 2006, Policy Services issued a Policy Update which provided a sample policy incorporating the requirements of the newly enacted *Information Security Breach and Notification Act*
Office of the New York State Comptroller issued an audit report titled *Security of Personal, Private and Sensitive Information (PPSI) in Mobile Computing Devices.*
School districts that subscribe to our Policy Update service received the revised and required policy on Information Security Breach and Notification (recommended #5672).

School districts that also subscribe to our Administrative Update service received a newly developed regulation, Data Breach Investigation and Notification Guidelines (recommended #5672R) and the updated New York State Security Breach Reporting Form (recommended #5672F) to assist district administrators in the implementation of the corresponding policy.
Summary of updated Policy and new Regulation:

- Definitions
- Determining if a Breach Has Occurred
- Investigation of Breaches
- Notification Requirements
- Methods of Notification
- Who Must Also Be Notified (names changed)
  - New York State Attorney General's Office
  - New York State Office of Cyber Security
  - New York State Department of State Division of Consumer Protection

An updated Form was also provided from the NYS Office of Cyber Security (used with permission).
• Personally identifiable information (PII) from student “education records”

• Major evolution in how PII is stored, processed and shared

Paper …… Electronic Data Systems Web Based Applications
FERPA

- Applies, whether student records are paper or electronic

  “Record means any information recorded in any way, including, but not limited to, handwriting, print, computer media, video or audio tape, film, microfilm, and microfiche.”

34 CFR 99.3
What is a Data Breach? (PTAC)

• Unauthorized disclosure occurs when:
  – personally identifiable information
  – from a student’s education record
  – made available to a third party who does not have legal authority to access the information

• Can happen inadvertently:
  – information about an individual is unintentionally revealed through a security breach of the electronic system that is used to maintain and access the education records, or
  – when a teacher or administrator accidentally leaves paper reports that include personally identifiable information in an unsecured location
Forms of Data Breach (PTAC)

• Hackers gaining access to data through a malicious attack;

• Lost, stolen, or temporarily misplaced equipment (e.g., laptops, mobile phones, portable thumb drives, etc.);

• Employee negligence (e.g., leaving a password list in a publicly accessible location, technical staff misconfiguring a security service or device, etc.);

• System failure (e.g., not requiring multiple overlapping security measures, failure of backup security measures, or the failure of a single protective system).
FIRPA

• Does NOT contain specific breach notification requirements

  – However, FERPA requires that school districts record each incidence of data disclosure

  34 CFR §99.32
• Letter to Paredes (2005)

• Commissioner of Higher Education (Texas) advised FPCO re: laptop containing student information was stolen

• FPCO praised steps taken to:
  – Immediately notify students, and assist in contacting credit bureaus
  – Report incident to local police department

• “Quick and thorough response serves as a model...”
• Letter to Goldstein (2006)

• Student searching her name on Google found link to CUNY portal

  – Link produced confidential financial aid reports of several hundred CUNY law school students, residing on CUNY’s content server
  – CUNY closed access to the list
  – Confidential information remained accessible on Google, by accessing Google’s stored HTML cached content
• “[I]f an educational agency or institution has experienced a theft of files or computer equipment, hacking or other intrusion, software or hardware malfunction, inadvertent release of data to Internet sites, or other unauthorized release or disclosure of education records, the Department suggests consideration of one or more of the following steps…….”

• “In any case, direct student notification may be advisable if the compromised data includes student SSNs and other identifying information that could lead to identity theft…..”
• New regulations were again silent on breach response and/or notification requirements (other than documenting the incident)

• Commentary in the Federal Register provided further insight regarding best practices in this area
In September 2012, PTAC developed a guidance document entitled the "Data Breach Response Checklist" to illustrate current industry "best practices" in data breach response and mitigation applicable to the education community.

School Districts that subscribe to our Policy Update Service received a sample policy on Student Data Breaches (recommended #7243) to address data breaches that specifically involve personally identifiable information (PII) of students. School districts were encouraged to use this suggested policy to explore and implement privacy and security "best practices," targeting its unique concerns and data systems.

School Districts that also subscribe to our Administrative Update Service received a sample regulation on Student Data Breaches: Prevention, Response and Notification (recommended #7243R). This regulation was developed to assist administrators in the implementation of the corresponding policy and offers more detailed guidelines for the prevention of student data breaches, and the suggested response and notification protocol should a student data breach occur.
NEW POLICY – Student Data Breaches (#7243)

• Defined student data breach;
• School districts have a legal responsibility to protect the privacy of education data;
• The District has implemented privacy and security measures designed to protect student data stored in its student data management systems;
• The Superintendent will develop and implement regulations for prevention, response and notification regarding student data breaches.
More detailed information to correspond to Policy:

- Definitions
- Prevention of Student Data Breaches
- Response to Student Data Breaches
- Notification of Student Data Breaches
- Consider Notification of FPCO and PTAC
When a breach of data occurs:

State Technology Law §208
(data elements such as SS#, driver’s license #, account or credit card number, when not encrypted, or when encryption key has been acquired)

FERPA
(records, files, documents, or other materials that contain information directly related to a student; and are maintained by the district or by a party acting for the district)
• Letter to Fagan (October, 2012)

• School attorney reported to FPCO that flash drive containing students’ education records went missing from a classroom
  – Did this constitute a “disclosure?”

• FPCO confirmed it was inadvertent disclosure

• “Should this office investigate a complaint or other indications of non-compliance, we would take into consideration what steps an educational agency has taken in response to a data breach…..
The U.S. Education Department's Privacy Technical Assistance Center (PTAC) is available to provide technical assistance on all FERPA related issues. They can be contacted at: www.ed.gov/ptac.

The U.S. Education Department's Family Policy Compliance Office (FPCO) can assist school districts with FERPA compliance issues. They can be contacted at: www.ed.gov/fpco.


Resources (continued)

State Longitudinal Data Systems and Student Privacy Protections Under the Family Educational Rights and Privacy Act
*Prepared for the Data Quality Campaign*
November, 2006
http://www.educationcounsel.com/docudepot/articles/pub.pdf

Data Stewardship: Managing Personally Identifiable Information in Student Education Records
IES National Center for Education Statistics. SLDS Technical Brief.
November 2010
Thank you for your time - Questions?

Colleen Sloan, Esq., Manager
Erie 1 BOCES, Labor Relations Service
Associate School Attorney
(716) 821-7410
Email: csloan@e1b.org

JoAnn Balazs, Director
Erie 1 BOCES, Management Services
(716) 821-7069
Email: jbalazs@e1b.org
Website: www.e1b.org

Janell Hallgren, Manager
Erie 1 BOCES, Policy Services
(716) 821-7084
(716) 821-7409 (fax)
Email: jhallgren@e1b.org
Website: www.e1b.org (Policy Services)