Managing the Privacy of Student Data

SETDA Leadership Summit
October 26, 2015
State Boards of Education Have At Least Some Authority Over Education Data Privacy
Managing the Privacy of Student Data

Paige Kowalski, Data Quality Campaign
Education is Changing

increasing data demands + evolving technology → need for new approaches for ensuring privacy
Focus of State and Federal Privacy Conversations

**Collection**
- How are data gathered?
- What types of data are gathered?
- Is parental consent needed?

**Access**
- Who can see these data?
- Who can use these data?
- Role-based access: Federal, State, District, Research.

**Sharing**
- Who can a school district or state export these data to?
- Implications for community partners, other agencies/sectors, researchers.
What does this mean for states?
110 bills related to student data privacy in 36 states
2015 State Legislative Activity

187 bills related to student data privacy in 47 states
“In Louisiana, a data privacy bill led to administrative headaches and potential inequities by requiring parent permission for students’ data to leave the district even for purposes such as determining college financial aid and scholarships.”

– The Washington Post
Georgia’s Student Data Privacy, Accessibility, and Transparency Act (SB 89)

- Combines provisions from many of last year’s most robust governance and transparency bills
- Covers state data, with the online service provider governance aspects of the SOPIPA law that California passed last year
  - Would prohibit service providers from using data for commercial purposes
- Protects student privacy and promotes the use of data to improve student achievement
What does this mean for Congress?
Federal Role in Safeguarding Student Data

• Ensure federal laws provide a strong foundation to protect student information

• Coordinate across agencies to provide clarity to schools as to how laws work together

• Support state and local capacity to safeguard data
Federal Student Privacy Activities in 2015

• FERPA Amendments (Rokita-Fudge)
  ▪ Access for research and community partners
• ESEA Reauthorization
  ▪ Student Data Privacy Policy Committee (Markey-Hatch)
  ▪ ITECH program with data literacy training
• Messer-Polis and Blumenthal-Daines Bills
  ▪ Use of student data by service providers
Student Data Principles
Data should…

1. Support student learning
2. Foster continuous improvement
3. Inform, engage, and empower
4. Be accessible to parents, students, and educators
5. Inform professional judgment of educators
6. Only be shared for authorized purposes
Everyone with access to student information should have...

7. Clear, publicly available rules
8. Access to only what they need
9. Training
10. Institutions that collect and maintain student information should have…

- Governance
- Transparency
- Security
- Communications
Stay updated!
StudentDataPrinciples.Org
#StudentDataPrinciples
Paige Kowalski
Paige@dataqualitycampaign.org
Data Security in a Digital World
Louisiana and PII Security
Personally Identifiable Information (PII)

Indirect PII
- Information that can be combined with other information to identify a specific individual

Direct PII
- Information that relates specifically to an individual
  (SSN, Name, Date of Birth)

Information that can be used to distinguish an individual
**Timeline**

- **Act 837 (2014)**
  - Data Sharing Agreement s Posted (1/1/15)

- **Act 677 (2014)**
  - Release of Secure ID (6/1/15)*
  - No release of PII to outside parties (6/1/15)*

- **Act 228 (2015)**
  - No release of PII moved to 8/1/15
  - Release of Secure ID moved to 8/1/15

* Modified by Act 228 (2015)
Act 837

- Prohibits LEAs from requiring the collection of non-academic data about students such as political affiliation, religious practices, or information.
- Restricts LEAs from sharing personally identifiable information (PII) about students with external entities, including LDE, starting June 1, 2015. The law provides limited exceptions:
  - LEAs may share students’ personally identifiable information with LDE if:
    - The parent has given written consent to share that information.
    - The state requires it for auditing, including enrollment counts.
  - LEAs may share PII with a private entity if they sign a data sharing agreement.
- Requires that all data sharing agreements be publicly posted.
- Defines PII as any two pieces of identifiable information. As such, first and last name are considered two pieces of identifiable information.
- Creation and release of Louisiana Secure ID for all students by June 1, 2015.
- All data sharing agreement with external vendors must be in place by June 1, 2015.
- Provides for up to $10,000 fine and/or 3 years in prison for illegal release of each identity.
Act 677

- Requires public posting of:
  - All PII data transfer agreements by Jan. 1, 2015
  - All new agreements must be posted within 10 days of signing
  - Profiles of each data recipient
  - List of all data transferred
  - Data Security Coordinator contact information
  - Process for filing a complaint
Act 837

**Benefits**
- Codifies what is and isn’t PII
- Mandates data and identity security
- Provided for a unified identifier for students

**Disadvantages**
- Very narrow window to comply with all aspects of the law
- Definition of PII very broad and amorphous
- Was subject to broadly differing interpretations by districts
- Made schools and districts inoperable due to restrictions
Act 677

**Benefits**
- Provided for transparency in data transfers and agreements surrounding them

**Disadvantages**
- Extremely short time frame to comply
- Required districts to renegotiate with vendors regarding data transfers
- Required extensive legal counsel and time to negotiate with some recalcitrant vendors
2015 Legislative Session

- Act 228
  - Clarifies language and narrows the definition of release of PII under Acts 837 & 677.
  - Changes date for end of data sharing without data transfer agreement from June 1, 2015 to August 1, 2015
  - Changes date of release of Louisiana Secure ID from June 1, 2015 to August 1, 2015
Act 228

Benefits

- Redefined, narrowed, and clarified definition of PII and the restrictions on it
- Moved dates for posting of data transfer agreements and issuance of Louisiana Secure ID to August 1, 2015

Disadvantages

- None
Securing Data

- Physical Security
- Data Sharing
- Secure ID
  - Data linkage
- Consent
Physical Security

- No access for unauthorized individuals
  - All data is secured in via encryption or physical barriers

- No “shoulder surfing”
  - Workers only allowed to access data on department owned devices and no sharing of devices

- Destruction of data
  - All data destroyed after use
  - All storage devices destroyed at end-of-life

- Secure transmittal
  - No fax transmittal
  - sFTP transfer only
Data Sharing

- All vendors must sign and adhere to updated data sharing agreements
- Data sharing agreements must comply with both federal and state laws
- Data sharing agreements must publicly posted
Secure ID

- All students issued a new state-wide Secure ID Number
  - No connection to any direct or indirect PII
  - Generated by state and issued to student at enrollment in public and non-public schools
  - Secure ID follows student throughout educational career, regardless of where they are enrolled
In order for student records to be secure, Secure ID is not linked to state student records and PII is not linked to local student records.

In order to link PII and Secure ID data, third party must do ID matchup.

Prevents any one entity from having all of the pieces.
Data Linkage

Third Party Performs Data Linkage

- School District Submits Secure ID
- State Submits PII
All voluntary data sharing must be consented to by parent (or student of majority age)

Includes:
- Transcripts to post-secondary institutions, scholarship, and financial aid programs
- All public news or publication entities including yearbook, school paper, graduation programs, etc.

Data includes:
- Student name
- Photos
- Grade information
- Racial information
- Classification information
Georgia’s Data Privacy Law
• SB89 introduced in 2015 legislative session
• Passed April 2015
• Signed into law May 2015
• Implementation date July 2016
• Resulted in 7 new Georgia laws
  – OCGA 20-2-660 to 20-2-667
Establish department-wide policies
Ensure student data privacy
Evaluate legislative and regulatory proposals
Conduct privacy impact study
Prepare annual report to General Assembly
Work with department General Counsel

Establish a department-wide Privacy Incident Program
Establish a model process and policy for any parent to file a complaint
Provide training, guidance, technical assistance and outreach to build a culture of privacy protection
The department shall develop model policies for local boards of education that:

<table>
<thead>
<tr>
<th>Support local boards of education in fulfilling their responsibility to annually notify parents of their right to request student information;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assist local boards of education with ensuring security when providing student data to parents;</td>
</tr>
<tr>
<td>Provide guidance and best practices to local boards of education in order to ensure that local boards of education provide student data only to authorized individuals;</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Support local boards of education in their responsibility to produce education records and student data included in such education records to parents and eligible students, ideally within three business days of the request; and</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assist schools and local boards of education with implementing technologies and programs that allow a parent to view online, download, and transmit data specific to his or her child's education record.</td>
</tr>
</tbody>
</table>
• The department shall develop model policies and procedures for a parent or eligible student to file a complaint with a local school system regarding a possible violation of rights under this article or under other federal or state student data privacy and security laws.

• Student personally identifiable data will not be transmitted to any federal, state, or local agency or nongovernmental organization except in certain situations.
Develop policies for the following:

- Criteria for the approval of research and data requests
- Restrictions on granting access to student data
- Prohibitions against publishing student data other than aggregate data or de-identified data in public reports
- Data retention and disposal policies
- Guidelines for authorizing access to the state data system
- Guidelines for authentication of authorized access
- To ensure the provision of at least annual notifications to eligible students and parents regarding student privacy rights under federal and state law.
Create and publish data inventory and dictionary

Notify Governor and General Assembly of:
  - New provisional student data - [Post for public comment for 60 days]
  - Changes to existing student PII data collections required for any reason including changes to federal reporting requirements made by USDOE.
  - List of special approvals granted by the GaDOE in the past year regarding release of student PII
  - Results of any and all privacy compliance and security audits completed in the past year.
Data Governance for Collections

Current Process

Data Collections Manager

- School Improvement
- Title I
- Special Education
- Title III/ESOL
- CTAE
- Budget
- Safe & Drug Free Schools

- Instructional Technology
- Policy
- Curriculum
- Assessment
- Accountability
- Title I Part D McKinney Vento

NOTE: Data manager meets with program areas to gather requirements

NOTE: Data manager shares requirements with SIS vendors, data specialists, developers, and database architects

Requirements Gathering → Collect Data → Data Validation → Superintendent Sign Off → Data Archived and Used
Data Governance for Collections

**NEW PROCESS**

Data Collections Manager

- School Improvement
- Title I
- Special Education
- Title III/ESOL
- CTAE
- Budget
- Safe & Drug Free Schools
- Instructional Technology
- Policy
- Curriculum
- Assessment
- Accountability
- Title I Part D McKinney Vento

**NOTE:** Data manager meets with program areas to gather requirements

**NOTE:** Data manager shares requirements with SIS vendors, data specialists, developers, and database architects

- Requirements Gathering
- 60 Day Comment Period
- Report to Governor & General Assembly
- Collect Data
- Data Validation
- Superintendent Sign Off
- Data Archived and Used
"Operator" means any entity other than the department, local boards of education, the Georgia Student Finance Commission, or schools to the extent that the entity:

A. Operates an Internet website, online service, online application, or mobile application with actual knowledge that the website, service, or application is used for K-12 school purposes and was designed and marketed for K-12 school purposes to the extent that it is operating in that capacity; and

B. Collects, maintains, or uses student personally identifiable information in a digital or electronic format.
An operator shall not knowingly:

• Use student data to engage in behaviorally targeted advertising

• Use information to amass a profile about a student except in furtherance of K-12 school purposes

• Sell a student's data

• Disclose student personally identifiable data without explicit written or electronic consent from a student over the age of 13 or a student's parent or guardian
Nothing in this Code section or this article prevents the department or local board of education and their employees from recommending, directly or via a product or service, any educational materials, online content, services, or other products to any student or his or her family if the department or local board of education determines that such products will benefit the student and does not receive compensation for developing, enabling, or communicating such recommendations.
Monitored NGFW – Advanced Endpoint Threat Detection

From March 1, 2015 to July 2, 2015 monitoring staff manually escalated a total of 104 security incidents.
3.2.2 Failure Rate

The failure rate on this campaign is the second highest of this quarter’s phishing emails. This phishing email attempts to get people to engage the phishing email.

14% of the recipients (55 of 405 recipients) clicked the link, which could have led to a data breach.

- Email Click: 14%
- Email View: 76%
- No Action: 10%

### Assignment Status

<table>
<thead>
<tr>
<th>Assignment Name</th>
<th>Overall Status</th>
<th>Not Started</th>
<th>In Progress</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q3 Remediation Training</td>
<td>In Progress</td>
<td>15%</td>
<td>0%</td>
<td>85%</td>
</tr>
<tr>
<td>Q3 Remediation Training</td>
<td>In Progress</td>
<td>20%</td>
<td>11%</td>
<td>69%</td>
</tr>
<tr>
<td>Q3 Remediation Training</td>
<td>In Progress</td>
<td>17%</td>
<td>3%</td>
<td>81%</td>
</tr>
</tbody>
</table>
• Incident Response
• Security Risk Consulting
• Monitored Infrastructure
• Monitored Next Gen Firewall
• Advanced Endpoint Threat Detection
• Managed Phishing Services
• Managed Advanced Malware Protection and Detection
• Identify system vulnerabilities
• Make sure you have the lay of the land (server, applications, users, etc.)
• Manage and prioritize risk
• Focus on detection and prevention
• Access
  ❖ Data (internal, external request)
  ❖ Database access
  ❖ HR (new hires and terminations/resignations, job change)
  ❖ ETC
• Penetration Test
  ❖ Internal and External
  ❖ Web Applications and Infrastructure

• Wireless Assessment
  ❖ Evaluated and Tested Each SSID
  ❖ Performed Pen Test

• Information Security Assessment
  ❖ Reviewed and Tested Agency’s Processes
  ❖ Access Controls
  ❖ Data Identification – Where is it
Advanced Endpoint Threat Detection

The Five Key Data Sources Collected From Sensors:
- Records of Execution
- Records of Filesystem Modifications
- Records of Registry Modifications
- Records of Network Connections
- A Copy of Every Binary Executed

And the relationship among all these data points:

Detect Threats As They Are Executed
Historic Visibility; Apply New Research To Previous Event Data
Lightweight Sensor | 3Mb Executable | <1% CPU, 10~Mb Ram
- On Demand Security Training
- Needs Assessment
- Program Development
- Customized Courses
Develop a detailed data security plan for the state data system that includes:

• Privacy and security audits;
• Plans for responding to security breaches, including notifications, remediation, and related procedures;
• Data security training and policies including technical, physical, and administrative safeguards;
• A process for evaluating and updating as necessary the data security plan, at least on an annual basis, in order to identify and address any risks to the security of student personally identifiable data; and
• Guidance for local boards of education to implement effective security practices that are consistent with those of the state data system.
Monitored Infrastructure

Client Remote Location
- Firewall
- IDS
- Server
- CTA Log Collector

Sophisticated Integration
- Standard Protocols
  - Syslog, SNMP, etc.
- Native APIs
  - Check Point OPSEC LEA
  - CISCO SDEE
  - Sourcefire e-Streamer
  - QualysGuard

Counter Threat Platform
- Purpose-built for MSS
  - Superior scalability
  - Advanced correlation across devices
  - Vendor-neutral monitoring

LogVault
Servers
iSensor
IDS/IPS
Applications
Firewall/VPN
Proxy
WAF

Client HQ Network

SOC Facilities
- Five Global SOC Locations
  - Real-time automated failover
- Experienced Security Experts
  - 24x7x365 support

CTU Intelligence
- Applied Research
  - Across global client base
- Latest Countermeasures
  - Protection from emerging threats

Portal and Reports

Internet

Counter Threat Unit Research Team
End-to-End IR Capabilities

Be Prepared for a Security Breach
- CSIRP Development
- Denial-of-Service Preparedness
- Advanced Threat Preparedness
- Compliance Integration
- CSIRP Gap Analysis
- Disclosure Planning
- Tabletop Exercises

Respond to a Security Breach
- Incident Handling
- Digital Forensics Investigation
- Incident Management
- Malware Analysis

Post-Incident Response
- Eradication & Recovery
- Postmortem Analysis
- Documentation
- Meet Legal, Regulatory and Compliance Reporting Requirements

Incident Response Retainer Services
- Teamwork
  - Infrastructure team
  - Legal

- Writing policies for standard operating procedures

- Gathering artifacts

- Developing privacy culture within the agency

- Expanding privacy conversation within the Data Governance Committee
What’s Coming Next?
Coming Soon

- More Laws and Regulations
- Accidental Consequences
- 1:1 Devices and Student Data Privacy
- Educator and Administrator Data
- Algorithms in Education
- Medical Data
- Student Discipline
- Biometrics