

Education Data Privacy

Ray Martin, Connecticut Department of Education

Susan Williams, Virginia Department of Education

Jan Petro, Colorado Department of Education

Connecticut

Where we were coming from?

- *Limited FERPA awareness*
- *Disjointed and contradictory data suppression rules*
- *Non-FERPA specific Data Sharing Agreement*

Improving General Awareness

Internal Efforts:

- **Reviews of past and current products**
- **FERPA as an ongoing Bureau and inter-bureau discussion point (especially with IT)**
- **Improved Data Governance**
- **FERPA Training**

External Efforts:

- **FERPA Training at Performance Office Annual Data Summit**
- **Data Confidentiality and Security as topics in Trainings and in materials**

Data Suppression

Historic Approach:

- Straight N counts
- Different data offices establishing their own standards
- Little to no coordination between offices
- Lack of awareness

Interim Point:

- N and Percentages
- Improved awareness
- Coordination between offices
- Uneven implementation

Data Suppression

Version 3.0 Approach:

- **N based suppression - Suppress when:**
 - **<20 for Assessment and accountability variables**
 - **≤ 5 for all others**
 - **Complimentary Suppression**
- **Computed Statistics**
 - **An N based with the Statistic has been suppressed**
 - **Numerator ≤ 5**
 - **Denominator <20**
 - **Extreme percentages converted to ranges (e.g., 0% proficient becomes <5% proficient)**

Data Sharing Agreement

The Old Connecticut State Department of Education (CSDE) data sharing agreement model was based upon financial data sharing agreements.

- ❑ Mentioned FERPA only to:
 - State why the sharing was permitted
 - Include language that the party receiving the data will follow FERPA.
- ❑ In the case of a breach by the party receiving the data, the contractor was required to offer credit monitoring of the students whose data were breached.
- ❑ Had little or no data protection requirements. Many of those that it did have were out of date.

Data Sharing Agreement Changes

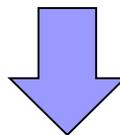
The new data sharing agreement model includes a number of new protections, many “best practice” items supported by PTAC and clarifies duties on both sides of the agreement. Big changes include:

- ❑ Infuses FERPA into the base of the agreement;
- ❑ Defines critical terms;
- ❑ Details data security standards;
- ❑ Outlines the data to be shared; and
- ❑ Makes specific changes in three key areas:
 - Data Protection
 - Data Suppression
 - Breach Protocols

Data Sharing Agreement Changes

Data Protection

“Password Protected Secure Environment”



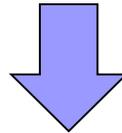
“For the purposes of this Agreement, data shall be deemed protected when on a secure server that is hosted by the Contractor and is password protected by a password that meets the following criteria:

- Contains at least 8 characters;
- Is comprised of at least 3 of the following 4 types of characters:
 - Lower case letters (i.e. a-z),
 - Upper case letters (i.e. A-Z),
 - Numbers (i.e. 0-9),
 - Special characters (e.g. !@#\$%^&*()_+|~); and
- Has not been used in the past year. “

Data Sharing Agreement Changes

Data Suppression

No language around data suppression existed. The general requirement to comply with FERPA was believed sufficient.

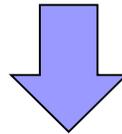


- Specific standards for suppression that match the CSDE's standards **AND**
- Contractually required CSDE review and approval period for all publications resulting from the data shared under the Agreement.

Data Sharing Agreement Changes

Breach Protocols

In case of breach (or a potential breach) a the contractor must inform the state, create a response plan and provide credit monitoring for student's whose data was breached.

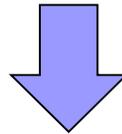


- Inform the state and make a response plan; **AND**
- Stop all use of CSDE data immediately;
- Pay a penalty of up to \$1,000 for each record breached;
- Be subject to Connecticut 5 year ban on receiving confidential data.

Data Sharing Agreement Changes

Breach Protocols – Outside Breaches

There was no requirement to inform the CSDE if the Contractor is banned in other states or districts.



Contractor is required to inform the CSDE of a non-CSDE data breach and cease using all CSDE provided data should it be banned by any organization from receiving PII. Furthermore, the Contractor agrees that they shall not resume use of the CSDE provided data without written authorization from the CSDE.

Connecticut State Level Efforts

State Confidentiality Regulations

For all state systems that collect or maintain confidential data, each Department must publish:

- System Name
- General Nature and purpose of the system
- Title and Address of Responsible Official
- Legal Authority for Collection, Maintenance and Use
- Types of Personal Data
- Uses of Personal Data
- Retention Schedule

Connecticut State Level Efforts

Public Act 10-142

“An Act Improving Data Security and Agency Effectiveness”

Revises state statutes that govern the sharing of data with contractors to set higher standards for data security. Contractors will need to:

- Implement and maintain a data-security program
- Implement, maintain and update security and breach investigation procedures
- Limit access to confidential data to only those employees with authorized need to access the data in completion of the contract
- Sets standards for the types of systems a contractor can use and methods acceptable for the transfer of confidential data

Next Steps/Challenges

We Have Much More to Do:

- ❖ Complete the automation of our data suppression rules
- ❖ Expanding FERPA and Privacy issues within the Department
- ❖ Set up Data Sharing Agreement website for public viewing
- ❖ Expanding the awareness of FERPA at the local level



Protecting Student Privacy in the Commonwealth of Virginia

Susan M. Williams

2015 Summer NCES Forum

Virginia Specific Privacy Laws

- § 22.1-287 – Limitations on access to records
- § 22.1-287.01 – Student information and release to federal government agencies
- § 22.287.1 – Directory information

Virginia Specific Privacy Laws

- § 22.1-288 – Furnishing information to public or private schools, colleges, or universities
- § 22.1-288.1 – Notation in school records of missing children

Virginia Specific Privacy Laws

- § 22.1-288.2 – Receipt, dissemination, and maintenance of records containing certain law-enforcement information
- § 22.1-289 – Transfer and management of scholastic records

VDOE Privacy Protections

- Cell suppression on public data sets
- Contract language
- Restricted use data agreements
 - How will the data be used ?
 - How will the data be secured ?
 - When will the data be destroyed ?
 - Who will have access ?
- Non-disclosure agreements

Additional Protections

- Multiple FOIA requests for similar data
- Teacher-Student Data Link (TSDL)
 - Longitudinal data
 - Publicly available third party materials
 - Small groups of students who have same schedules need to be suppressed

VLDS Privacy Video



Colorado Strong Privacy Protections

Jan Rose Petro
Director of Data Services
Colorado Department of Education

Data Privacy and Security

- Data is foundation to business of education
- The Colorado Department of Education takes seriously its obligation to protect the privacy of data
 - Collected
 - Used
 - Shared
 - Stored
- Historically, have protected data

EIMAC Data Privacy & Security Subgroup - Technical

Privacy means...

We have control over the data we manage/own – data governance defines rules for managing our data, so if in place, allows us that control

Security means...

There is freedom from risk (of data breach, id theft, use of personal data for harm) – putting procedures and systems in place to protect data

Privacy vs. Security



Privacy – Determination of: what money goes into the bank, what money gets moved, who receives the money after it's moved, how much goes, keeping the money out of the wrong hands



Security – armoring the truck, determining logistics of moving money from one place to another, maintaining the truck's engine/tires/etc., protecting money in bank, guarding the bank vaults, etc.

Impetus for Strengthening

- Parent concerns
- State Board desire for transparency
- Legislative action

Bringing Privacy to the Forefront

- Data Management Committee
- Executive team interest
- CDE wide effort
- Reliance on other experts/organizations
- HB 14-1294 Student Data Privacy Act

HB 14-1294 Student Data Privacy Act

- Provide data dictionary
- Develop and publish policies and procedures
 - FERPA and other privacy laws
 - Restrict CDE access
- Data sharing agreements
- Data security plan
- Ensure FERPA compliance
- Vendor contract language to safeguard privacy and security
- Process to review all data requests
- CDE can't require data unless mandated by federal or state law (grants excepted)
- Specifies data not to be collected by CDE
- Publish vendors
- Develop security guidance for LEAs

Actions to Augment Privacy

- CDE employee awareness/training
- CDE privacy-related policies/practices
- Appoint privacy team
- Strengthen website

CDE Employee Awareness/Training

- CDE Employee Data-Sharing and Confidentiality Agreement
- Annual Security Awareness Training
 - Includes PTAC's FERPA 101 and Data Sharing 201
- Self-identified CDE research and evaluation employees
 - "National Institute of Health, Office of Extramural Research, *Protecting Human Research Participants*" training
- April 2015 PTAC training

CDE Privacy-related Policies/Practices

- CDE Enterprise Data Governance Policy
- Information Security and Privacy Policy
- Strengthening Data Security Assurances with additional information security requirements
 - Contracts
 - Data sharing agreements
- Data Privacy and Security Protocols
 - Review procedures for agreements involving personally identifiable information (PII)
 - Data collection and protection procedures
 - Process for parents requesting student-level information
 - Confidentiality agreements and training for CDE Staff
- Data Privacy-Related Guidance for Districts

Appoint Privacy Team

- Chief Privacy Officer
- Chief Information Officer
- Information Security Officer
- Meet biweekly
 - Review contracts
 - Examine data sharing agreements
 - Discuss issues

Strengthen Website: Key Points

- Had some privacy items prior
 - Scattered
- Executive commitment
- CDE-wide effort
- Communications involvement
- Privacy team support
- Data foundational
 - Obligation to protect
 - List of CDE major data collections

Strengthen Website: Guidance for Districts and Schools

- Information for Parents
 - How Education Data Is Used
 - FERPA General Guidance for Parents
 - About the Family Policy Compliance Office-U.S Dept. of Education (FPCO)
 - A Parent's Guide to Student Data Privacy - FERPA | SHERPA
- Who Uses Student Data?
 - DQC Video and Infographic
- General Resources
 - District Guidance on Student Information Security and Privacy Data Collection Opt Out Requests
 - Best Practices for Keeping Parents Informed About Student Data Collection
 - The Privacy of Student Information: A Resource for Schools-National Forum on Education Statistics
 - Frequently Asked Questions
- Tools
 - Data Dictionary
 - Toolkit for Navigating Federal Privacy and Security Laws
 - Pledge to Safeguard Student Privacy

Strengthen Website: Federal Laws and Policies

- Children's Online Privacy Protection Act (COPPA)
- Family Educational Rights and Privacy Act (FERPA)
- Protection of Pupil Rights Amendment (PPRA)
- Uninterrupted Scholars Act

Strengthen Website: State Law and Policies

- CDE Information Security and Privacy Policy (January 2014)
 - staff training on data use
 - security breaches
 - personally identifiable student data
 - requirements for data sharing agreements
- HB 14-1294 Student Data Privacy Act
- CDE Data Security Assurances

Strengthen Website: Data Privacy and Security Procedures

- Review Procedures for Agreements Involving Personally Identifiable Information (PII)
 - Visual: Review and Approval Process
 - Definitions and Review Processes with contract template
 - CDE Data Request Form
 - Checklist for Agreements Involving Personally Identifiable Information
 - Review Process: Agreements Involving Personally Identifiable Information
 - CDE Inter-Office Agreements Involving Personally Identifiable Information
- Data Collection and Protection Procedures
 - State-Level Student Data Collection and Protection (January 2014)
- Process for Parents Requesting Student-Level Information
- Confidentiality Agreements and Training for CDE Staff

Strengthen Website: Agreements

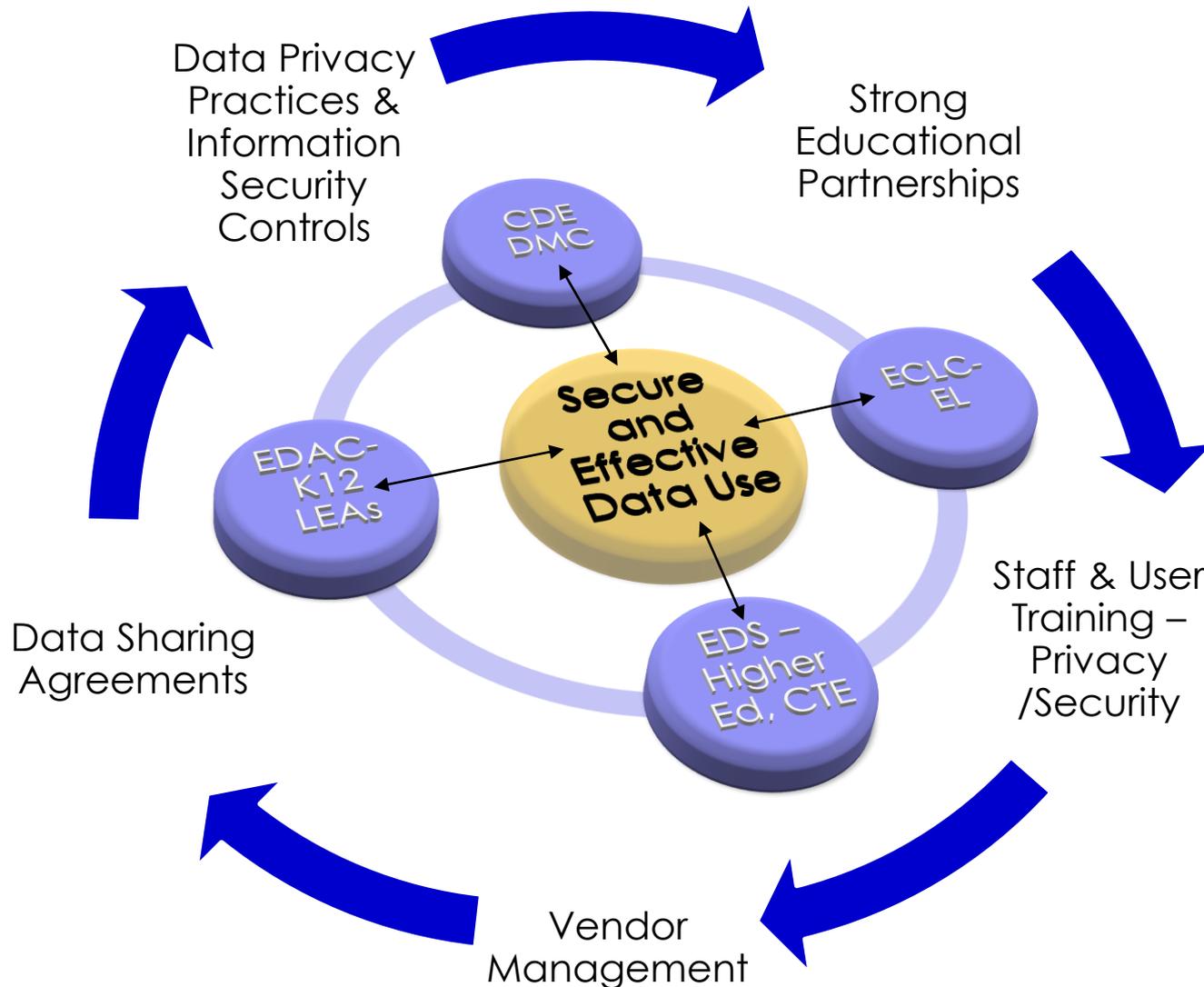
- Post vendor contracts beginning May 2014
- Agreement Title
- Agreement Type
- Attachments
- Date Approved
- Purpose of Agreement

Strengthen Website: Research and Reports

- Reports and Documents on Student Data Privacy and Security
 - PTAC
 - Fordham University

- Organizations Involved with Student Data Privacy and Security
 - Consortium for School Networking
 - Data Quality Campaign
 - Education Privacy Information Center (EPIC)
 - FERPA | SHERPA
 - Fordham Center on Law and Information Policy
 - Privacy Technical Assistance Center (PTAC)
 - USDOE Family Policy Compliance Office: Resource Website

Operational Data Management



Critical Success Factors

- Executive team support
- CDE wide focus, including Communications
- Designated Chief Privacy Officer
- Privacy team
- Wealth of other privacy expertise/materials

Foundations for the Future

- Chief Privacy Officer
- Continued transparency
 - Website
 - Vendor contracts
- Detailed data sharing agreements
- Established Data Governance Program