COLORADO
Department of Education

Data Privacy Protections in Contracts

JUNE 10, 2015

Proposed Process

June	SBE provides guidance on general concepts to include; CDE solicits input from parents and other stakeholders on new contract provisions
July	CDE continues to solicit input on new contract provisions
August	SBE approves template for new contract provisions; CDE begins including new provisions in contracts

Incorporating New Contract Requirements

1. **Identify all contracts involving student PII.**
2. **Prioritize new contracts and contracts scheduled for renewal within the next year.**
3. **In instances where CDE is legislatively mandated or there is no alternative vendor to enter into contracts, flexibility may be necessary.**
   - Commissioner will have discretion to negotiate terms.
   - CDE will publicly post information about contracts that do not include all new contract provisions.

CDE Contracts
Current Status

1. CDE has amended most contracts to require privacy and security protections.
2. CDE contracts that disclose or use Student Data are currently listed on the CDE website. https://www.cde.state.co.us/dataprivacyandsecurity/agreements
3. New contract template will build upon existing privacy and security protections and include additional protections consistent with the Board policy directive.

Stakeholder Input

1. **Solicit stakeholder input on privacy concerns with vendor contracts.**
   A. Parents
   B. Vendors
   C. School Districts Representatives
   D. Other Members of the Public
2. **Hold a public meeting to provide all interested parties with an opportunity for input.**
3. **Publicly post the new contract template to amend contracts for additional privacy and security protections. Field input from interested parties.**

Legislative History

1. HB 14-1294 established privacy and security requirements for the Department and Department contracts that disclose Student PII.
2. Department supported SB 15-173 – it would have provided the Department with statutory authority to mandate additional privacy and security requirements in vendor contracts.
3. The Department has completed a side-by-side comparison of the Senate and House versions of SB 15-173 and is proposing to implement the strictest privacy protections and most onerous requirements on vendors.

Specifying Authorized Users, Data Used and Purpose

Current Requirements

- Designate the individual that will serve as the authorized representative for the provided services or the individuals that will be directly responsible for managing the data in question.
- Specify the purpose for which the PII is being disclosed.
- Specify the student information that will be disclosed.
- Describe how the student information will be used and why disclosure of PII is necessary to carry out the work authorized in the contract.

Potential Additions from SB 15-173

Vendor may not use any PII from any source unless it has demonstrated a specific legitimate educational purpose for doing so and the use has been expressly authorized in the CDE contract.

Limiting Use of Data

Current Requirements

Require the authorized representative to use PII only to meet the purpose of the disclosure as stated in the written agreement and not for commercial purposes or further disclosure.

Potential Additions from SB 15-173

Specify that vendor may not target advertisements to students if targeting is based on student information acquired because of a student's or parent's use of the vendor's website, service or application.

Vendor may not use information acquired through its website, services or applications to create a personal profile of a student that is not in furtherance of educational purposes set forth in CDE contract.

Specify that vendor may not sell any student information obtained as a result of vendor's contract with CDE, unless vendor is sold to, acquired by, or merged with another vendor, provided that the successor entity continues to comply with all of the data privacy protections outlined in CDE's data sharing contract.

Limiting Use of Data (Cont.)

Current Requirements	Potential Additions from SB 15-173
Require the authorized representative to use PII only to meet the purpose of the disclosure as stated in the written agreement and <u>not for commercial purposes or further disclosure.</u>	Vendor <u>may not disclose</u> any personally-identifiable information obtained as a result of vendor's contract with CDE <u>except</u>: • In furtherance of the educational purpose of the vendor's website, service or application; • To protect the security and integrity of the vendor's website, service or application; • To take precautions against liability; • To respond to the judicial process;

Limiting Use of Data (Cont.)

Current Requirements

Require the authorized representative to use PII only to meet the purpose of the disclosure as stated in the written agreement and <u>not for commercial purposes or further disclosure.</u>

Potential Additions from SB 15-173

- To the extent required by other provisions of law, to provide information to law enforcement agencies or for an investigation on a matter related to public safety; or
- To a service provider, provided that the vendor contractually prohibits the service provider from using the PII for any purpose other than providing the contracted service, prohibits further disclosure of the information except as necessary to carry out the legitimate educational functions delegated to the service provider, and requires the service provider to implement and maintain reasonable security procedures and practices.

Data Retention

Current Requirements	Potential Additions from SB 15-173
Require the PII to be <u>destroyed when the information is no longer needed</u> for the purpose specified and specify a time period for destruction. (Note: agreement may indicate that parties can agree to later make an amendment that will extend the time period, if needed.) Require the authorized representative to provide written confirmation to CDE when the education records have been destroyed, per the terms of the agreement.	Vendor must agree to delete student information at the request of a school or LEA.

Security Policies and Procedures

Current Requirements	Potential Additions from SB 15-173
Require appropriate technical, physical, and administrative safeguards to protect PII data at rest and in transit. Examples of this include secure-file transfer protocols ("SFTP"), hyper-text transfer protocol over secure socket layer ("HTTPS") and encryption. Require policies and procedures to protect PII from further disclosure and unauthorized use, including limiting use of PII to only the authorized representatives with legitimate interests in performing work authorized by the contract.	None

Security Policies and Procedures (Cont.)

Current Requirements	Potential Additions from SB 15-173
Verify that the authorized representative has a sound data security program to protect data at rest and in transmission including specific required data security provisions, including requirements related to encryption, where the data can be hosted, transmission methodologies, and provisions to prevent unauthorized access. The agreement may include the requirement that the authorized representative provide certification indicating that an independent vulnerability or risk assessment of this data security program has occurred or include the right for CDE to physically inspect the authorized representative's premises or technology used to transmit or maintain data. Verify that the authorized representative has in place a data stewardship plan with support and participation from across the organization that details the organization's policies and procedures to protect privacy and data security, including the ongoing management of data collection, processing, storage, maintenance, use, and destruction.	None

Right to Audit

Current Requirements	Potential Additions from SB 15-173
CDE has the right to conduct audits or other monitoring activities of the authorized representative's data stewardship policies, procedures, and systems. If, through these monitoring activities, a vulnerability is found, the authorized representative must take timely appropriate action to correct or mitigate any weaknesses discovered. CDE has the right to review any data prior to publication and to verify that proper disclosure avoidance techniques have been used and to approve reports prior to publication to ensure they reflect the original intent of the agreement.	None

Transparency

Current Requirements	Potential Additions from SB 15-173
None	Vendor must: • Post contact information for the entity collecting or generating student information and any third party to whom it has disclosed information; • Post type of student information that is collected or generated by the vendor or disclosed to a third party; • Post the educational purpose(s) for which the student information is used; • Post its policies regarding retention and disposal of student information; • Post information about the types of information collected and how the operator shares and uses it; • Upon request, provide LEAs with information about the specific data elements that are collected or generated, the vendor's security policies, and any other data that is merged with the student data that it collects or generates; • Provide notice before making changes to its privacy policies; and • Facilitate students' and parents' access to and correction of student information.

Breaches

Current Requirements	Potential Additions from SB 15-173
Include a plan for how to respond to any breach in security, including the requirement that any breach in security must be reported immediately to CDE. Include penalties for noncompliance. Verify that the authorized representative has appropriate disciplinary policies for employees that violate the privacy or security requirements of the contract, including termination in appropriate instances.	An interested party may report alleged violations to the Department. Develop a process for public comment on changes to the contract template and post notice of intent to bid out certain vendor contracts.

Defining Protected Data

Current Requirements

Protected information is defined as Personally Identifiable Information under FERPA and Student Data under C.R.S. 22-2-309(2)(e)

Personally Identifiable Information (PII) includes, but is not limited to:

- **the student's name;**
- **the name of the student's parent or other family members;**
- **the address of the student or student's family;**
- **a personal identifier, such as:**
  - ✓ **the student's social security number,**
  - ✓ **student number,**
  - ✓ **biometric record;**
- **other indirect identifiers, such as:**
  - ✓ **the student's date of birth,**
  - ✓ **place of birth,**
  - ✓ **mother's maiden name;**

Other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

Defining Protected Data (Cont.)

Current Requirements

PII also means a dataset that is linked to a specific individual and that would allow a reasonable person in a school community, who does not have knowledge of the relevant circumstances, to identify the individual with reasonable certainty.

"Student Data" means data that is collected and stored by CDE at the individual student level and is included in a student's educational record and includes:

- **State-administered assessment results, including:**
  - **participation information,**
  - **courses taken and completed,**
  - **credits earned and other transcript information;**
- **course grades and grade point average;**
- **grade level and expected graduation year;**
- **degree, diploma credential attainment or other school exit information;**
- **attendance and mobility information between and within Colorado school districts;**
- **special education data and special education discipline reports limited to object information that is sufficient to produce the federal Title IV annual incident report;**
- **date of birth, full name, gender, race, and ethnicity;**
- **program participation information required by state or federal law.**

Defining Protected Data (Cont.)

Potential Additions from SB 15-173

Protected information includes PII that is created or provided by a student, parent or employee of an LEA, or gathered by a vendor by use of a website that personally identifies a student including:

- **an electronic mail address,**
- **cell phone number,**
- **any other information that allows physical or on-line contact**

Protected information includes:

- **discipline or criminal records**
- **juvenile dependency**
- **medical or health records**
- **biometric information**
- **disabilities**
- **socioeconomic information**
- **political affiliations**
- **religious information**
- **text messages**
- **student identifiers**
- **search activity**
- **photos**
- **voice recordings**
- **food purchase**
- **geolocation information**