



COLORADO
Department of Education

May Public Meeting

Data Privacy

May 24, 2016

Agenda

- **New Data Privacy Law**
- **Research Data Request for PII Vetting Process**
- **Public Comment**



COLORADO
Department of Education

New Data Privacy Law

New Data Privacy Law - Overview

- **Name of Law:** Student Data Transparency and Security Act
- **Summary:** The bill adds to the existing laws pertaining to student data security by adopting additional duties that the State Board of Education (State Board), Department of Education (CDE), and School Districts, Boards of Cooperative Services, and Charter Schools (LEPs) must comply with to increase the transparency and security of the Student Personally Identifiable Information (Student PII) that CDE and the LEPs collect and maintain. The bill imposes duties on the commercial entities that provide school services by formal contract with CDE or an LEP (Contract Providers) and the commercial entities that an LEP or employees of an LEP choose to use without entering in a formal, negotiated contract (On-Demand Providers).

New Data Privacy Law – Implementation Timelines

- On or after effective date (**August 10, 2016**) – CDE and LEPs cannot enter into or renew a contract with entities that refuse to accept terms of updated contracts and provisions of the bill.
- **March 1, 2017** – CDE must create and make available sample student information privacy and protection policy for LEPs.
- **December 31, 2017** – LEPs to adopt a student information privacy and protection policy.
- **July 1, 2018** – Small rural districts to adopt a student information privacy and protection policy.
- **This bill is extremely complicated and analyzing all impacts of the bill's language will take some time. Please visit CDE's Privacy and Security website regularly to follow our progress.**
<https://www.cde.state.co.us/dataprivacyandsecurity>

New Data Privacy Law – Definitions

- "Student Personally Identifiable Information" (Student PII) means information that, alone or in combination, personally identifies an individual student or the student's parent or family, and that is collected, maintained, generated, or inferred by a public education entity, either directly or through a school service, or by a school service contract provider or school service on-demand provider. [22-16-103 (13), C.R.S.]

New Data Privacy Law – Definitions cont.

- "Destroy" means to remove Student Personally Identifiable Information so that it is permanently irretrievable in the normal course of business. [22-16-103 (3), C.R.S.]

New Data Privacy Law – Definitions cont.

(a) "School Service" means an internet website, online service, online application, or mobile application that:

(I) is designed and marketed primarily for use in a preschool, elementary school, or secondary school;

(II) is used at the direction of teachers or other employees of a Local Education Provider; and

(III) collects, maintains, or uses Student Personally Identifiable Information.

(b) "School Service" does not include an internet website, online service, online application, or mobile application that is designed and marketed for use by individuals or entities generally, even if it is also marketed to a United States preschool, elementary school, or secondary school. [22-16-103 (7), C.R.S.]

New Data Privacy Law – Definitions cont.

- "School Service Contract Provider" or "Contract Provider" means an entity, other than a Public Education Entity or an institution of higher education, that enters into a formal, negotiated contract with a Public Education Entity to provide a School Service. [22-16-103 (8), C.R.S.]
- "School Service On-Demand Provider" or "On-Demand Provider" means an entity, other than a Public Education Entity, that provides a School Service on occasion to a Public Education Entity, subject to agreement by the Public Education Entity, or an employee of the Public Education Entity, to standard, non-negotiable terms and conditions of service established by the providing entity. [22-16-103 (9), C.R.S.]

New Data Privacy Law – Transparency in Data Collection

- **Requirement:** Create, publish, and make publicly available a data inventory and dictionary or index of data elements with definitions of individual student data fields used in the student data system. [22-16-104 (1)(a), C.R.S.]
- CDE currently posts a data inventory of elements collected within its student data system. That list is located here:
<https://www.cde.state.co.us/dataprivacyandsecurity/dataelementscollected>
- CDE will continue to maintain this information.

New Data Privacy Law – Privacy Policies and Procedures

- **Requirement:** Develop, publish, and make publicly available policies and procedures to comply with the federal "Family Educational Rights and Privacy Act of 1974", 20 U.S.C. sec. 1232g, and other relevant privacy laws and policies, including but not limited to policies that restrict access to Student PII in the student data system. [22-16-104 (1)(b), C.R.S.]
- CDE currently posts its Information Security and Privacy Policy on its public website. It's located here:
<https://www.cde.state.co.us/cdereval/cdeinformationsecurityandprivacypolicy>
- CDE will work to make any necessary updates required by the contents of the new law.

New Data Privacy Law – Transparency for Data Transfers

- **Requirement:** CDE shall publish and maintain on its website a list of all of the entities or individuals, including but not limited to vendors, individual researchers, research organizations, institutions of higher education, and government agencies, that CDE contracts with or has agreements with and that receives or uses Student PII and a copy of each contract or agreement.

[22-16-105(4), C.R.S.]

- CDE currently posts all vendor, research and interagency data sharing agreements involving Student PII to its public website. This page will be updated to comply with the requirements of the new bill.
- Current link:
<https://www.cde.state.co.us/dataprivacyandsecurity/agreements>

New Data Privacy Law – Public Hearing for Vendor Breaches

- **Requirement:** If the contract provider commits a material breach of the contract that involves the misuse or unauthorized release of Student PII, CDE shall determine whether to terminate the contract in accordance with a policy adopted by the State Board. At a minimum, the policy must require the State Board, within a reasonable time after CDE identifies the existence of a material breach, to hold a public hearing that includes discussion of the nature of the material breach, an opportunity for the contract provider to respond concerning the material breach, public testimony, and a decision as to whether to direct CDE to terminate or continue the contract. [22-16-105(5)(b), C.R.S.]
- CDE will work with the State Board of Education to develop this policy and create a process for holding public meetings in the event of a vendor contract breach.

New Data Privacy Law – Parent Complaint Process

- **Requirement:** The governing board of each LEP shall adopt a policy for hearing complaints from parents regarding the LEP's compliance with the requirements of this article. At a minimum, the policy must provide a parent the opportunity to submit information to the governing board and receive a hearing by the governing board and must require the governing board to take action on the parent's complaint within sixty days after the hearing. [22-16-112(2)(a), C.R.S.]
- **Requirement:** If a LEP does not comply with the requirements specified in this article, a student's parent may submit a complaint to the governing board of the LEP. [22-16-112(2)(b), C.R.S.]

New Data Privacy Law – District Obligations

- Each Local Education Provider (LEP) will need to post on their website clear information about the data elements that are collected and maintained in their data systems. [22-16-107(1)(a), C.R.S.]
- Each LEP will need to:
 - Post and maintain a list of all school service contract providers that involve PII that the LEP contracts with and post a copy of the contract. [22-16-107(1)(b), C.R.S.]
 - Update their current contract terms to comply with the requirements of the new law. [22-16-107(2)(a), C.R.S.]
 - Post a list of all on-demand service providers that involve PII that the LEP uses and, on the request of a parent, review the provider's compliance with the requirements of the new law. [22-16-107(3)(a), C.R.S.]
 - Adopt a student information privacy and protection policy, post that policy to its website and make it available to parents on request. [22-16-107(4)(a), C.R.S.]
- Should an on-demand service provider not comply with its privacy policy or the requirements of the new law, the LEP is strongly encouraged to stop using that provider and post on its website a list of all on-demand service providers that it has stopped using. The LEP will need to post a notice of this procedure on its website. [22-16-107(3)(c), C.R.S.]

New Data Privacy Law – Vendor Obligations

- Vendors can only collect, use or share PII for the purposes stated in the contract. If they want to use the data in another way, they must get consent from the parent or student if over age 18. [22-16-109(1)(a), C.R.S. and 22-16-109(1)(b), C.R.S.]
- Vendors and their subcontractors must:
 - Provide on their website and provide to public education entities information explaining the Student PII they collect and how that data is used and shared. [22-16-108(1), C.R.S.]
 - Update each public education entity with notice before making material changes to its privacy policy. [22-16-108(2), C.R.S.]
 - Provide access to and correction of any factually inaccurate information. [22-16-108(3), C.R.S.]
 - Notify the contracting public education entity of any misuse or unauthorized breach of Student PII upon its discovery. [22-16-108(4), C.R.S.]

New Data Privacy Law – Vendor Obligations cont.

- Vendors cannot:
 - Sell Student PII. [22-16-109(2)(a), C.R.S.]
 - Use Student PII for the purposes of targeted advertising. [22-16-109(2)(b), C.R.S.]
 - Use Student PII to create a personal profile of the student outside of the requirements of the contract or with the consent of the student or parent. [22-16-109(2)(c), C.R.S.]
- A vendor can only share Student PII with a subcontractor provided that they contractually obligate the subcontractor to comply with the requirements of this law. [22-16-109(3)(b), C.R.S.]
- Each vendor must maintain a comprehensive information security program. [22-16-110(1), C.R.S.]
- A vendor must destroy Student PII upon the request of the public education entity. [22-16-110(2), C.R.S.]
- A vendor must destroy Student PII upon the termination of the contract according to the timelines established by that contract or when the data is no longer needed for the performance of the contract. [22-16-110(3), C.R.S.]

New Data Privacy Law – CDE Support for Districts

- CDE will develop data security guidance for LEPs. [22-16-106(1), C.R.S.]
- CDE will provide LEPs with sample student information privacy and protection policies. [22-16-106(2), C.R.S.]
- CDE will provide LEPs with sample contract language for use in contracting with vendors and keep this language up-to-date in light of advances in data technology. [22-16-106(3), C.R.S.]
- CDE will make available to LEPs resources that they can use in training their employees in privacy and security. [22-16-106(4), C.R.S.]
- On the request of a LEP, CDE will provide the LEP with training related to student information security and privacy. [22-16-106(4), C.R.S.]
- Upon receiving information that an LEP has stopped using a vendor due to the misuse of PII, CDE will post that information to its public website. [22-16-106(5), C.R.S.]



COLORADO

Department of Education

PII Data Request Process for Researchers

PII Request Process for Research - Overview

- CDE takes the transfers of Personally Identifiable Information to third parties very seriously.
- CDE has an existing process in place to evaluate requests from researchers to use Colorado student's PII.
- CDE's contracts with researchers already include most of the requirements of the new bill, including:
 - Ensure that contracts with researchers include the scope, purpose and duration of the study and the PII that will be disclosed.
 - Ensure that researchers use PII only for the purposes stated in the research agreement.
 - Require the study to be conducted in a way that does not reveal the identities of student involved in the research.
 - Require the researcher to destroy all PII at the end of the study.
- CDE will continue to refine this process based on the requirements of the new bill and guidance from the State Board of Education and the Commissioner.

PII Request Process for Research – Current Process

- CDE starts the data request for research process via a form available on the CDE website:
<https://www.cde.state.co.us/research/researchanddatarequests>
 - The form requires detailed information from the researcher on the sponsoring entity (usually an institution of higher education) and all researchers that will be participating in the study.
 - The form requires the researcher to identify the purposes for the receipt of data from CDE under the requirements of FERPA.
 - The researcher must identify in detail the specific data being requested, the research proposal, the justification, the methodology, the reason why PII must be used, and any funding sources.
 - The researcher must provide CDE with copies of the following:
 - Institutional Review Board (IRB) approval for the use of PII.
 - The CV and qualifications of the researchers and advisors.
 - Documentation of the completion of data security training.

PII Request Process for Research – Current Process cont.

- Once CDE receives this documentation, CDE consults with internal staff (including data custodians) to determine if the research proposal should be accepted. The following items are considered as part of this vetting process:
 - Is the research FERPA and statute compliant? If the answer to either of these is “no”, the researcher is told that CDE cannot fulfill this request.
 - Is the researcher in good standing on any previous projects?
 - What is the significance of research proposal?
 - Is the research of specific benefit to CDE?
 - Does the research align with CDE’s and the Board of Education’s strategic priorities?
 - What is the validity of the research plan (is the researcher qualified, are the methods appropriate)?
 - What are the data elements specified? Do we want to share those data elements with the researcher? Are any data elements sensitive in any way?
 - Has IRB approval been provided?
 - Has the data security training documentation been provided?
- Provided that the internal staff approves the research, they present the research to the Commissioner and the State Board of Education for their approval.

PII Request Process for Research – Current Process cont.

- Once approved by the Commissioner and the State Board of Education, CDE works with the researcher to put in place a Research Data Sharing Agreement that includes the following:
 - Strict controls around how the researcher can use data.
 - Stringent security and privacy protections that must be in place to protect the data.
 - Requirements for the researcher to provide CDE with the results of the research.
 - Requirements for the researcher to destroy the data once the research has been completed on a schedule specifically listed in the Research Data Sharing Agreement.
 - Research Data Sharing Agreements must comply with the requirements of the new law applicable to vendors.
- Research Data Sharing Agreements are reviewed on an annual basis, should the research extend beyond a year.
- Once the term of the Data Sharing Agreement has reached its end, CDE follows up with the researcher to obtain the results of the research and to gain a confirmation that the data has been destroyed.



COLORADO
Department of Education

Public Comment

Public Comments

- CDE will now be taking public comments from attendees.
- Answers to questions will not be provided during the meeting.
- We will compile answers to everyone's questions and post them on our Privacy and Security website along with a copy of this presentation at:
<https://www.cde.state.co.us/dataprivacyandsecurity>.
- This meeting must end at 4 PM, so the Public Comment period may be cut short. Please help us to manage the time by the following:
 - If you know of others that have the same topic, please coordinate with them to allow for others to present their topics.
 - Please be respectful of others and limit your comments to 3 minutes.
- If you have additional questions or don't have an opportunity to comment, please send your questions and concerns to dataprivacy@cde.state.co.us.