COLORADO DEPARTMENT *of* EDUCATION

Review and Approval Procedures:

Agreements Involving Personally Identifiable Information

June 2014

CDE PII Review Team
201 E. Colfax Ave., Denver, CO 80203

Contact:
Elliott Asp, Ph.D.
Special Assistant to the Commissioner of Education
Phone: 303-866-6868
Email: Asp_e@cde.state.co.us

Table of Contents

Executive Summary

The Colorado Department of Education, (CDE or Department), is required by law to collect and store student and educator records, and takes seriously its obligations to secure information systems and protect the privacy of data collected, used, shared and stored by the Department. For more information, see the "State-Level Student Data Collection and Protection document located at http://bit.ly/1qje5oC. CDE's commitment to secure and protect data privacy includes the development of guidelines and a review process for agreements that involve the sharing of personally identifiable information (commonly abbreviated as PII) between units within the Department, with external entities and for research purposes.

Please Note: Local Education Agencies (LEAs), which are typically school districts and BOCES cooperatives, routinely provide CDE data, some of which includes PII. A formal agreement is not required in this instance because LEAs are required to report this data under state statute.

This packet contains the documents that make up that review process. The packet includes:

- PII Definitions and Review Processes
- Approval Process: Agreements Involving PII
- Data Request Form
- Interoffice PII Agreement
- Checklist for Agreements Involving PII

As a rule, CDE does not share PII. However, under federal and state law there are specific circumstances in which the sharing of PII is allowable and, in some cases, required (see the CDE Information Security and Privacy Policy document located at http://bit.ly/1qje5oC for more information). Within the parameters of federal and state statute there are several different types of agreements that could involve the sharing of PII the Department has collected. Generally, these fall into three categories: data sharing agreements with other state agencies, contracts with vendors for particular services, and providing data to institutions and individuals for research purposes. The review/approval process for these different types of agreements involving PII differ according to the type of agreement. These agreements and the review process for each are described in detail in the PII "Definitions and Review Processes" and the "Approval Process: Agreements Involving Personally Identifiable Information" documents.

All agreements in which PII is to be shared must be approved through the appropriate process before being signed by the Commissioner or his designee. On May 1, 2014, CDE instituted its data and security review processes. All contracts or agreements involving PII entered into, amended or extend on or after May 1 are posted on CDE's Data Privacy and Security webpage (http://bit.ly/1qje5oC)[1]. As Agreements involving PII are approved, they will be added to the webpage.

This document will be reviewed and updated regularly. Please check for the most current version on CDE's Data Privacy and Security web page at http://bit.ly/1qje5oC.

For more information and/or questions about the approval process and the agreements that are in force, contact Elliott Asp, Special Assistant to the Commissioner at 303-866-6868 or asp_e@cde.state.co.us.

[1] If an agreement is more than 75 pages long, only the data security provisions will be posted. However, the entire agreement can be viewed by contacting the CDE Communication Office.

Definitions and Review Processes: Agreements involving PII

All agreements involving PII undergo rigorous review at CDE. This section is a reference to define types of agreements that might involve PII , defines what "Use of PII" means, and describes the review processes for each agreement type.

Definitions

- **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, or biometric record; other indirect identifiers, such as the student's date of birth, place of birth, and 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.

- 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.

Types of Agreements

1. **Data Sharing Agreements (DSAs) -** Agreements that are created between CDE and another state agency (such as the Department of Higher Education) for the purpose of sharing data to fill a statutory requirement, perform cross-departmental research, or produce aggregated reports on remediation or post-secondary enrollment.

2. **Research Agreements -** Agreements between CDE and individuals and institutions who wish to conduct research using Colorado student or school system data already collected by CDE. This includes doctoral and master's degree candidates, university faculty, independent researchers, and private and public agencies.

3. **Contracts** are legally binding agreements with specific terms between two or more persons or entities in which there is a promise to do something in return for a valuable benefit known as "consideration."

Defining "Use of PII"

Any agreements that involve the disclosure of PII are thoroughly examined through CDE's review and approval process. Specific directions and obligations pertaining to PII are explicitly articulated in every individual agreement and contract.

Review Processes for Each Agreement Type:

Data Sharing Agreements

- Agreement submitted to CDE's PII Review Team.
- Requirements in the "Checklist for Agreements Involving PII" (page 13) are met so that the agreement is in compliance with CDE policy.
- Data privacy language is added to all agreements involving disclosure of PII.

Research Agreements

- Proposal submitted to CDE's Institutional Review Board (IRB) (http://www.cde.state.co.us/research/irb).
- Once approved, sent to CDE's PII Review Team.
- Requirements in the "Checklist for Agreements Involving PII" (page 13) are met so that the agreement is in compliance with CDE policy.
- Data privacy language is added to all agreements involving disclosure of PII.

Contracts

- All contracts are based on a template (http://bit.ly/1qje5oC) which has been reviewed and approved by the Attorney General's Office, Governor's Office of Information Technology (OIT) and the Colorado State Controller's Office.
- Data privacy procedures are included in all contracts involving disclosure of PII.
- Contracts are negotiated to ensure PII is protected in accordance with both CDE's and OIT's Data Security and Privacy Policies and the CDE "Checklist for Agreements involving PII" (page 13).
- The Commissioner will be notified of any concerns about contractual issues relating to PII which cannot be resolved during negotiations.
- The Commissioner approves all contracts before they are executed.

Approval Process: Agreements Involving PII

Purpose

This document is used by CDE staff when developing and reviewing agreements involving the disclosure of PII .

Please note that when data is shared between offices or units within CDE rather than to outside entities, CDE staff members need not apply the following review process and are instead required to complete the "CDE InterOffice Agreements Involving PII" document (page 8-10).

Determining Need for Review

Any agreements that involve the disclosure of PII are thoroughly examined through CDE's review and approval process. Specific directions and obligations pertaining to PII are explicitly articulated in every individual agreement and contract. The process varies depending on the type of agreement/document (page 5).
This includes agreements:

- Data Sharing Agreements (DSAs)
- Research Agreements
- Contract Agreements

CDE Internal Review Process

Directions for Staff

Before having an agreement involving PII reviewed, utilize the "CDE Checklist for Agreements Involving PII" to ensure the agreement meets all requirements listed (page 13).

Note: The CDE staff member who submits the agreement is referenced below as "submitter".

After the checklist requirements are met:

1. Send the agreement to Margo Allen at allen_m@cde.state.co.us and let her know if there is a requested deadline for the agreement to obtain signatures and to be submitted. She will forward the agreement to CDE's PII Review Team (Please Note: Review can take from one to several weeks depending on the nature and content of the agreement. Allow as much time as possible for review).

2. Margo will log the agreement in a central database to track progress of review.

3. Margo will submit the agreement to the appropriate review staff (see list below).

4. Margo is the main point of contact regarding progress updates.

5. **If there are no changes after review:**
The submitter will be notified by a member of the PII Review Team that the agreement has been approved (copy Margo).

- The staff member that is to sign the approved agreement (and his/her assistant, if applicable) will be copied on the email.

- Once signed, an electronic copy will be sent to the submitter and Margo Allen who will share it with the PII Review Team and electronically file the signed agreement. Signed agreements need to also be filed with the CDE office involved with the agreement. The original document will be returned to the submitter. It is up to the submitter's discretion whether a hard copy or electronic copy must be kept on file.
- Once the agreement is approved and signed, it is the submitter's responsibility to share the final agreement with the outside entity.
- Once fully signed, the agreement will be posted on the Data Privacy and Security web page (http://www.cde.state.co.us/cdereval/agreementsinvolvingpii).

6. **If there are necessary changes after review:**
   - A member of the PII Review Team will contact the staff member who submitted the agreement to discuss (copy Margo).
   - The submitter will work with the outside entities involved to make the necessary changes, then re-submit the document to the member of the PII Review Team (and copy Margo) for final approval. Once approved, see #5.

CDE's PII Review Team

All data sharing agreements involving PII will be reviewed by the following internal team:

- **Review Team Lead:** Elliott Asp, Special Assistant to the Commissioner
- Dan Domagala, Chief Information Officer
- Marcia Bohannon, Deputy Chief Information Officer
- Kady Lanoha, Senior Policy Associate
- Janelle Asmus, Chief Communications Officer and/or Amy Skinner, Director of Communications
- TBD, Information Security Officer
- **Logistics Lead:** Margo Allen

Depending on the type and contents of the agreement, additional reviewers may be necessary.

- Dan Jorgensen: Research Agreements
- Trish Bohm: Contracts
- Tony Dyl and/or Sally Pennington, Attorney General's Office (Elliott Asp will determine)
- Other content specialists, as needed

CDE Data Request Form

Purpose: This form must be filled out for any type of data request. This includes both request that do and requests that do not involve PII.

Date:_____

Person Requesting Information:_____

Affiliation and Address: _____

Phone Number: _____ **Email Address:** _____

Requested information: (If the information you are requesting is available on the CDE web site the department will ask you to use the data located there. Please refer to the end of this document for a list of web locations which may contain the data you are requesting). **Note: CDE will blank out data with student counts of less than 16 students on all data requests. This is to ensure that student confidentiality is maintained. When making your request, please keep this in mind.**

Grade level to be included in data request _____

Content Areas to be included in data request _____

Years to be included in data request _____

Other Information:

Purpose: (This information will assist us in meeting your request.)

Level of detail: (Do you want your analysis in percentages or numbers, scale scores or performance levels? Which demographic variables would you like?

How would you like this information? ☐ Electronic Copy (Be sure to provide an email address.)
☐ Hard Copy (Please provide a mailing address.)

In what format would you like your analysis? (i.e., Excel spreadsheets)

Date information is needed: _____

Have you checked the CDE website for this information? ☐ **YES** ☐ **NO**
If not please visit www.cde.state.co.us/index_assess.htm before submitting this form. The information you are requesting may be found on the website. See the end of this document for a list.

Note: If your request involves disclosure of PII to another CDE Office or an outside entity, **additional information is required**. PII is 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.
-If you are a **CDE Office** you must fill out the Inter-Office Agreement Involving PII: http://bit.ly/1qje5oC-If you are an **outside entity** you must address information in the Checklist for Agreements Involving PII: http://bit.ly/1qje5oC

If you have a question as to whether you are requesting PII, contact Dennis St. Hilaire (st.hilaire_d@cde.state.co.us) and he will connect you with the Data Owner so this can be verified.

It is recommended that you use individual but de-identified data, instead of PII, for your request if at all possible.

TO BE COMPLETED BY CDE STAFF:

CDE Authorization:_____ Priority Level: ☐ Low ☐ High

CDE staff responding to the request: _____ Date and name information was released: _____

Format of analysis: _____

CDE Interoffice Agreements Involving PII

This form must be signed any time an office at CDE is requesting PII from another CDE office. This is not necessary for data requests that do not disclose PII or for data that is available on the CDE website. The data may only be used for the purpose(s) stated in this document. Both offices should keep the signed agreement on file. Also send a signed copy to Margo Allen at allen_m@cde.state.co.us.

Note: This agreement is to be reviewed annually if this is an ongoing request. The original agreement is valid until there is a request for it to be changed.

Date:

Contact Name/CDE Office Requesting Data:

Contact Name/CDE Office Sharing Data:

Contact Name/CDE Office Data Owner:

What data is being requested?

Explain how the data will be used by the requesting office:

Explain how the data will be securely stored or destroyed before, during and after use by the requesting office:

Will the data be shared with any staff outside of the requesting office? Please verify that the data will not be shared outside of CDE:

I authorize the requesting office to have access to the data requested above.

_____ _____ _____ _____

Supervisor Signature (Sharing Office) Date Data Owner Signature Date

_____ _____

Printed Name Printed Name

Checklist Agreements Involving PII

Purpose

This section is to be used by staff of CDE when developing and reviewing agreements involving the disclosure of PII to **outside entities**, such as contracted vendors/organizations or other state agencies.

Please note that, when data is shared between offices or units within CDE rather than to outside entities, CDE staff members need not apply the following checklists and are instead required to complete the "CDE InterOffice Agreements Involving PII" document (page 8-10).

Because this document will be reviewed and updated on a regular basis, please check for the most current version of the document on CDE's Data Privacy and Security web page at http://bit.ly/1qje5oC.

The Educational Studies Exception

The **Educational Studies Exception** in FERPA and CDE's Data Security and Privacy Policy allows CDE to disclose PII without parental consent to organizations conducting studies ***for, or on behalf of, CDE***. These studies can only be for the purpose of developing, validating, or administering predictive tests; administering student aid programs; or improving instruction. For instance, CDE may disclose PII (without prior consent) to an organization that CDE has asked to conduct a study to compare program outcomes across school districts to assess which programs provide the best instruction and in order to duplicate those results in other districts. Please note that the Department's Institutional Review Board reviews and authorizes all disclosure agreements under the Educational Studies Exception.

Under the Educational Studies Exception, written agreements **must:**

- □ Specify the purpose of the study to be conducted;
- □ Specify the scope or breadth of the proposed study;
- □ Specify the duration of the study;
- □ Specify the information to be disclosed in order to conduct the study;
- □ Specify the research methodology that will be used and why disclosure of PII is necessary to accomplish the research;
- □ Designate the individual that will serve as the authorized representative for the study or the individuals that will be directly responsible for managing the data in question;
- □ 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 for further disclosure;
- □ Require the authorized representative to conduct the study in a manner that does not permit the personal identification of parents and students by anyone other than those with a legitimate need to know to complete the study;

- □ Affirms that the authorized representative may only publish results in a way that protects the privacy and confidentiality of the individuals involved. For example, when publishing tables, cell suppression and other methods of disclosure avoidance must be used so that students cannot be identified through small numbers displayed in table cells;

- □ Requires the authorized representative to destroy the PII from the education records when the information is no longer needed for the purpose specified and specifies 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.) Requires the authorized representative to provide written confirmation to CDE when the education records have been destroyed, per the terms of the agreement;

- □ Outlines appropriate technical, physical and administrative safeguards to protect PII data at rest and in transit. Examples of this include secure-file transfer protocols ("SFTP") and hyper-text transfer protocol over secure socket layer ("HTTPS");

- □ Includes 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;

- □ Verify that the authorized representative has a sound data security program to protect data at rest and in transmission. This may be addressed through language in the agreement that states what data security provisions are required, 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. The agreement may also include the right for CDE to physically inspect the authorized representative's premises or technology used to transmit or maintain data. If the data is shared with an individual, he or she must comply with CDE's data security program;

- □ 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. If the data is shared with an individual, he or she must comply with CDE's data stewardship plan;

- □ Verify that the authorized representative has appropriate disciplinary policies for employees that violate FERPA, including termination in appropriate instances. If the data is shared with an individual, he or she must be willing to submit to CDE's disciplinary policies for employees that violate FERPA;

- □ State that 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; and

- □ State that 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.

The Audit or Compliance Activities Exception

The **Audit or Compliance Activities Exception** in FERPA and CDE's Data Security and Privacy Policy allows CDE to disclose PII, without consent, to authorized representatives of contracted vendors/organizations or other state agencies. PII must be used to audit or evaluate a federal or state supported ***education program***, or to enforce or comply with federal legal requirements that relate to those education programs (audit, evaluation, or enforcement or compliance activity). For example, CDE may share PII, without consent, to authorized representatives of another state agency for purposes of evaluating the effectiveness of and reporting outcomes for a particular educational grant program.

Under the Audit or Compliance Activities Exception, written agreements **must:**

- ☐ Designate the individual that will serve as the authorized representative for the audit/evaluation or the individuals that will be directly responsible for managing the data in question;
- ☐ Specify the purpose for which the PII is being disclosed and specifically states that the disclosure is in furtherance of an audit, evaluation or enforcement or compliance activity;
- ☐ 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 audit, evaluation, or enforcement or compliance activity;
- ☐ Requires 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;
- ☐ Require the PII to be destroyed when the information is no longer needed for the purpose specified and specifies 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.) Requires the authorized representative to provide written confirmation to CDE when the education records have been destroyed, per the terms of the agreement;
- ☐ Outline appropriate technical, physical and administrative safeguards to protect PII data at rest and in transit. Examples of this include secure-file transfer protocols ("SFTP") and hyper-text transfer protocol over secure socket layer ("HTTPS");
- ☐ Outline policies and procedures to protect PII from further disclosure and unauthorized use, including limiting use of PII to only the authorized representatives with a legitimate interests in the audit, evaluation, or enforcement or compliance activity;
- ☐ 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;
- ☐ Verify that the authorized representative has a sound data security program to protect data at rest and in transmission. This may be addressed through language in the data sharing agreement that states what

data security provisions are required 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. The agreement may also include the right for CDE to physically inspect the authorized representative's premises or technology used to transmit or maintain data. If the data is shared with an individual, he or she must follow CDE's data security program, and submit to physical inspections conducted by CDE as necessary;

- ☐ 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. If the data is shared with an individual, he or she must comply with CDE's data stewardship plan;

- ☐ Verify that the authorized representative has appropriate disciplinary policies for employees that violate FERPA, including termination in appropriate instances. If the data is shared with an individual, he or she must be willing to submit to CDE's disciplinary policies for employees that violate FERPA;

- ☐ State that 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; and

- ☐ State that 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.