COLORADO DEPARTMENT of EDUCATION

Checklist for Data Sharing Agreements

Purpose

This document is intended to be used by staff of the Colorado Department of Education (CDE) when developing and reviewing agreements involving the disclosure of *personally identifiable student information* (PII) to *outside entities*, such as contracted vendors/organizations or other state agencies. PII 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. 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 Inter-Office Data Sharing Agreement located at: http://mycde.cde.state.co.us/generalresources/datasharing.

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://www.cde.state.co.us/cdereval/dataprivacyandsecurity.

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;

cde

- ☐ 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;

- ☐ When data is shared with an entity rather than an individual, 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;

- ☐ When data is shared with an entity rather than an individual, 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;

- ☐ When data is shared with an entity rather than an individual, verify that the authorized representative has appropriate disciplinary policies for employees that violate FERPA, including termination in appropriate instances;

- ☐ When data is shared with an entity rather than an individual, 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 personally identifiable information to only the authorized representatives with a legitimate interests in the audit, evaluation, or enforcement or compliance activity;

cde

- ☐ 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;

- ☐ When data is shared with an entity rather than an individual, 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;

- ☐ When data is shared with an entity rather than an individual, 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;

- ☐ When data is shared with an entity rather than an individual, verify that the authorized representative has appropriate disciplinary policies for employees that violate FERPA, including termination in appropriate instances;

- ☐ When data is shared with an entity rather than an individual, 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.