COLORADO DEPARTMENT of EDUCATION

Information Security and Privacy Policy

Overview

The Colorado Department of Education (CDE or Department) is required by law to collect and store student and educator records[1], and takes seriously its obligations to secure information systems and protect the privacy of data collected, used, shared and stored by the Department. Educational data is an asset that is essential to CDE's business and must be diligently protected. In accordance with Colorado Revised Statutes, section 22-2-307, CDE has adopted the policies below to ensure that it is fully compliant with and also exceeds the requirements of the Family Educational Rights and Privacy Act (FERPA) and its other legal and regulatory obligations.

Process for Maintaining the Information and Security Privacy Policy

In conjunction with the U.S. Department of Education's Privacy Technical Assistance Center and the state Education Data Advisory Committee, CDE annually monitors changes in state and federal regulations that are related to data collection and reporting and updates CDE procedures to address any new requirements and best practices. For instance, FERPA was recently reauthorized (in January 2012) to include additional clarity around and support for the development and use of statewide longitudinal data systems. CDE's policies and procedures have been reviewed by CDE staff, legal counsel, and independent policy experts to ensure that they fully align with these revised federal regulations.

Technology Security Practices

As required by section 24-37.5-404, C.R.S., CDE maintains an annually-updated, confidential information security policy and plan. This includes an annual, independent risk assessment and vulnerability audit by an outside entity. CDE also monitors all access and access attempts to all of its data systems and maintains a centralized authentication and authorization process to further track access and safeguard its data.

Staff Training

In order to minimize the risk of human error and misuse of information, CDE provides a range of training opportunities for all staff using educational data.

All new CDE employees and contracted partners must sign and obey the CDE Employee Acceptable Use Policy, which describes the permissible uses of state technology and information. New CDE employees and contracted partners also must sign and obey the CDE Employee Data Sharing and Confidentiality Agreement, which describes appropriate uses and the safeguarding of student and educator data. Employees are required to participate in an annual information security and privacy fundamentals training, which is mandatory for continued access to the Department's network.

Additionally, CDE requires targeted information security training for specific groups within the agency and provides updated guidance to local education agencies concerning compliance with state and federal privacy laws and best practices in this ever-changing environment. For instance, CDE expects that all personnel engaged in program evaluation

[1] For information about what student records entail, please see CDE's fact sheet, "State-Level Student Data Collection in Colorado."

and/or research activities complete online training on the ethical and professional standards for protecting human research participants.

Data Retention and Disposition

The personally identifiable student information that CDE is legally required to collect is maintained according to the retention and disposition schedules outlined by the Colorado State Archives in its *State Agency Records Management Manual*. See https://www.colorado.gov/pacific/sites/default/files/StateRecordsManagementManual.pdf. For information defined as "Student Permanent Record" (i.e., demographics, enrollment and academic performance data), CDE archives this personally identifiable information and protects it with appropriate technical, physical, and administrative safeguards in accordance with FERPA. For "non-permanent" student information (i.e., audit workpapers or voluntary survey data), CDE deletes or destroys this information upon expiration of the retention period outlined in the *Records Management Manual*.

Internal Use of Data

The personally identifiable information from students' and educators' education records that CDE receives from LEAs and schools for audit, evaluation, or compliance purposes is not available to all CDE employees. This information is only available to employees and contract partners who have a reasonable and appropriate need for access to the information in order to maintain the records or to assist in conducting CDE evaluation, audit, or compliance functions and who have undergone a background check. The Department's Data Management Committee is comprised of data owners and coordinators at CDE who help ensure that data is properly handled from collection to reporting. This committee assists in identifying the CDE employees who have a legitimate need for access to data and developing policies concerning the management of the department's data. The committee also provides the commissioner with an up-to-date list of the specific individuals within the department who have the ability to link personally identifiable student information. For more information, see CDE's Data Governance webpage.

Breaches in Security

Concerns about security breaches must be reported immediately to the Department's Chief Information Officer. If the Chief Information Officer, in collaboration with the commissioner and appropriate members of the Department's executive team, determines that one or more employees or contracted partners have substantially failed to comply with the Department's information security and privacy policies, they will identify appropriate consequences, which may include termination of employment or a contract and further legal action. Concerns about security breaches that involve the Chief Information Officer must be reported immediately to the commissioner. The commissioner will collaborate with appropriate members of the Department's executive team to determine whether a security breach has occurred and will identify appropriate consequences, which may include termination of employment or a contract.

Disclosure of Educator Data

The Department is responsible for several activities that require the collection of data for licensed educators in Colorado. As the entity responsible for issuing and renewing educator licenses, linking student achievement to practicing educators, and monitoring implementation of local educator evaluation systems, CDE must manage and secure information that is sensitive and confidential. The Department maintains several statutory and regulatory protections to keep educator data private.

As required by section 22-2-111, C.R.S., all papers filed at CDE that contain personal information about holders of educator licenses or authorizations are classified as confidential. Each educator has the right to inspect and to have copies

made (at the educator's expense) of all information pertaining to the educator. Educators may challenge any such record by formal letter or other evidence, which shall be added to CDE's records. The information may be shared in the normal and proper course of administering licenses and authorizations, but it is otherwise unlawful for any CDE employee or other person to divulge, or make known in any way, any such personal information without the written consent of the educator. Personnel information may be published in the aggregate, so long as the identities of individual educators remain anonymous and the data pool is large enough to prevent the identification of individual educators, which in no instance shall be smaller than five educators.

Section 22-9-109, C.R.S. clarifies that, while CDE may collect information concerning an individual educator's performance evaluation ratings and student assessments results linked to the educator in order to fulfill its duties as required by law, this information must remain confidential and may not be published in any way that would identify the individual educator. CDE is authorized to share this data for research purposes, so long as the data is collected per established protocol and is used in a manner that protects the identity of the educator. The State Board of Education's rules concerning the evaluation of licensed personnel (1 CCR 301-87), in section 6.04(B) further clarify that CDE shall only publicly report data related to performance evaluation ratings in the aggregate at the school-, district-, and state-level, and shall not publicly report this data for cohorts smaller than five educators.

Disclosure of De-identified Student Data

CDE may disclose de-identified student data through the process outlined by the department's Institutional Review Board (IRB). The IRB considers and reviews all requests to conduct research using Colorado student or school system data already collected by CDE. Potential users such as doctoral and master's degree candidates, university faculty, independent researchers, and private and public agencies must submit proposals before receiving data and conducting and publishing their research.

Based on each data request, the department's IRB ensures that any data shared is "de-identified" (so that individual students are not personally identifiable). For instance, data may be considered "de-identified" if a meaningless code has been attached to each student's record in a way that prevents any student's identity from being identified or the data has been aggregated into a large enough pool of data that a student's identify cannot be inferred.

Those requesting data must meet all of the IRB's criteria prior to obtaining access to any de-identified student-level data from CDE. One of these criteria is that the researchers have completed training on the ethical and professional standards for protecting human research participants that is either the same as or equivalent to the training that CDE employees complete.

For more information about how de-identified student data may be disclosed, see the CDE Institutional Review Board Application.

Disclosure of Personally Identifiable Student Data

In compliance with the Family Educational Rights and Privacy Act (FERPA), CDE does not disclose personally identifiable information from student records unless the disclosure is for one of the limited purposes outlined in FERPA, 34 CFR § 99.31, including the following.

- Student Transfer and Enrollment: Student information may be disclosed, subject to the requirements of FERPA, 34 CFR § 99.34, to officials of another school, school system, or institution of postsecondary education where the student seeks or intends to enroll, or where the student is already enrolled so long as the disclosure is for purposes related to the student's enrollment or transfer and the student's former district has provided prior notification of this service through its annual FERPA notification letter.

- Educational Studies: Student information may be disclosed to organizations conducting studies for, or on behalf of, CDE to: (1) develop, validate, or administer predictive tests; (2) administer student aid programs; or (3) improve instruction. Disclosures for the purposes of such studies must ensure that the study is conducted in a manner that does not permit personal identification of parents and students by individuals other than representatives of the organization that have legitimate interests in the information, the information is destroyed when no longer needed for the purposes for which the study was conducted, and CDE enters into a written agreement that meets the requirements outlined below.

- Audits or Compliance Activities: Student information may be disclosed to authorized representatives of CDE in connection with an audit or evaluation of Federal or state supported education programs, or for the enforcement of or compliance with Federal legal requirements that relate to those programs. Disclosures for the purposes of such audits, evaluations, or compliance activities must ensure that CDE uses reasonable methods to ensure that its authorized representative: (1) uses personally identifiable information only to carry out an audit or evaluation of Federal- or State-supported education programs, or for the enforcement of or compliance with Federal legal requirements related to these programs; (2) protects the personally identifiable information from further disclosures or other uses, in accordance with FERPA; (3) destroys the personally identifiable information in accordance with FERPA; and (4) CDE enters into a written agreement that meets the requirements outlined below.

Requirements for Data Sharing Agreements to Disclose Student Data for Studies on Behalf of CDE

Prior to sharing personally identifiable student information for purposes of educational studies for or on behalf of CDE, CDE must enter into a written agreement or contract that meets the following requirements:

- Designates the individual or entity that will serve as the authorized representative. If an entity is designated, the agreement must specify the individuals directly responsible for managing the data in question;

- Specifies the purpose, scope and duration of the study and the information to be disclosed. This description must include the research methodology and why disclosure of personally identifiable information from education records is necessary to accomplish the research. Note, CDE will not disclose all of the personally identifiable information from its education records; rather, it will determine only the specific elements the authorized representative needs and disclose only those;

- Requires the authorized representative to use personally identifiable information only to meet the purpose of the disclosure as stated in the written agreement and not for commercial purposes or further disclosure. Approval to use the personally identifiable information from the education records for one study, audit, or evaluation does not confer approval to use it for another;

- Requires 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 representatives of the organization with legitimate interests. The agreement must require the authorized representative to conduct the study so as to not identify students or their parents. This typically means that the authorized representative should allow internal access to personally identifiable information from education records only to individuals with a need to know for the purposes of the study, and that the authorized representative should take steps to maintain the confidentiality of the personally identifiable information at all stages of the study, including within the final report, by using appropriate disclosure avoidance techniques;

- 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 personally identifiable information from the education records when the information is no longer needed for the purpose specified and must be clear about how the education records will be destroyed. The agreement must identify a specific time period for destruction based on the facts and circumstances surrounding the disclosure and study. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit. The agreement shall also require the authorized representative to provide written confirmation to CDE when the education records have been destroyed, per the terms of the contract;

- Documents appropriate technical, physical, and administrative safeguards to protect personally identifiable student 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");

- The agreement establishes policies and procedures to protect personally identifiable student information from further disclosure and unauthorized use, including limiting use of personally identifiable information to only the authorized representatives with a legitimate interests in the research or study; and

- 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.

Requirements for Data Sharing Agreements to Disclose Student Data for Audits, Evaluation or Compliance Monitoring

Written agreements for audits, evaluation or compliance monitoring are similar to, but slightly different than, agreements for research and studies. These written agreements or contracts must include the following requirements:

- Designates the individual or entity that will serve as the authorized representative. If an entity is designated, the agreement must specify the individuals directly responsible for managing the data in question;

- Specifies the purpose for which the personally identifiable student information from education records is being disclosed and state specifically that the disclosure is in furtherance of an audit, evaluation, or enforcement or compliance activity. The agreement must specify the student information to be disclosed and must include a description of how the student data will be used. The agreement must describe the methodology and why disclosure of personally identifiable student information is necessary to carry out the audit, evaluation, or enforcement or compliance activity;

- Requires the authorized representative to use personally identifiable information only to meet the purpose of the disclosure as stated in the written agreement and not for commercial purposes or further disclosure;

- Requires the authorized representative to destroy the personally identifiable information from the education records when the information is no longer needed for the purpose specified and must be clear about how the education records will be destroyed. The agreement must identify a specific time period for destruction based on the facts and circumstances surrounding the disclosure and study. The parties to the written agreement may agree to amend the agreement to extend the time period if needed, but the agreement must include a time limit.

The agreement shall require the authorized representative to provide written confirmation to CDE when the education records have been destroyed, per the terms of the agreement;

- Documents appropriate technical, physical, and administrative safeguards to protect personally identifiable student 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");

- The agreement establishes policies and procedures to protect personally identifiable student information 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; and

- 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.

Monitoring Implementation of Data Sharing Agreements

In addition to all of the precautions addressed above, any data sharing agreement or contract shall also address the following assurances to protect personally identifiable information from further disclosure and unauthorized use:

- CDE shall 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. CDE may require the authorized representative to provide a certification indicating that an independent vulnerability or risk assessment of this data security program has occurred. CDE shall also maintain the right to physically inspect the authorized representative's premises or technology used to transmit or maintain data;

CDE shall 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. CDE may also wish to verify that the authorized representative has a training program to teach its employees about FERPA and how to protect personally identifiable information from education records.

- If applicable, CDE shall verify that the authorized representative has appropriate disciplinary policies for employees that violate FERPA, including termination in appropriate instances;

- CDE shall maintain 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

- CDE shall maintain the right to review any data prior to publication and to verify that proper disclosure avoidance techniques have been used and shall maintain the right to approve reports prior to publication to ensure they reflect the original intent of the agreement.

Consequences for Failure to Comply with Data Sharing Agreements

An individual may file a written complaint with CDE regarding an alleged violation of a data sharing agreement or contract. A complaint must contain specific allegations of fact giving reasonable cause to believe that a violation of a data sharing agreement or contract has occurred. CDE will investigate all reasonable and timely complaints. CDE may also conduct its own investigation when no complaint has been filed or a complaint has been withdrawn, to determine whether a violation has occurred.

As required by FERPA, if an authorized representative that receives data to perform evaluations, audits, or compliance activities improperly discloses the data, CDE shall deny that representative further access to personally identifiable data for at least five years. In addition, CDE may pursue penalties permitted under state contract law, such as liquidated damages.

Additional Resources

CDE maintains and enforces a series of other policies related to information security, including:

- *State-Level Student Data Collection and Protection*;
- *CDE Guidelines for Data Requests*; and
- *District Guidance: Information Security and Privacy*.

Additional resources related to the collection, storage and safeguarding of student and educator information, including links to resources published by Education Privacy Information Center, the Data Quality Campaign, Fordham Center on Law and Information Policy, and the Privacy Technical Assistance Center, are available at http://www.cde.state.co.us/cdereval/dataprivacyandsecurity.