Research Data Sharing Agreement between the Colorado Department of Education (CDE) and the The Board of Trustees of the Leland Stanford Junior University, on behalf of the Center for Research on Education Outcomes

This Research Data Sharing Agreement (Agreement) is entered into by and between the Colorado Department of Education (CDE), 201 E. Colfax Avenue Denver, CO 80203 and The Board of Trustees of the Leland Stanford Junior University, on behalf of the Center for Research on Education Outcomes (CREDO), whose address is 434 Galvez Mall, Stanford University, Stanford, CA 94305-6010 ("Requester"), each individually a Party and together the Parties.

I. Scope of Agreement

CDE is a State Education Agency responsible for the implementation of education laws adopted by the State of Colorado. In fulfillment of law found in the Colorado Revised Statutes, CDE is charged with collecting and securely maintaining data on students enrolled in the state's Local Education Agencies (LEAs).

This Research Data Sharing Agreement applies to all data sharing between Requestor and CDE. Specific data to be shared are outlined in attached appendices, along with the purpose of data sharing, data ownership and conditions and/or regulations governing the usage of the shared data, requirements for shared data retention/destruction, and Party processes for implementing these actions.

II. Purpose

CDE and Requestor enter into this Agreement effective on June 15, 2016 to share and exchange Data for the purposes of conducting studies for, or on behalf of, educational agencies or institutions to develop, validate, or administer predictive tests; administer student aid programs; or improve instruction.

This Agreement is designed to be an umbrella agreement for all data sharing activities between CDE and Requestor. For each specific use case, i.e., detailed data requests for specific research purposes, the details shall be spelled out in the Appendix attached to this Agreement. The appendices will include the specific data requested and disclosed and the particular use of the data;

- The roles of the Data Provider (defined below) and Data Consumer (defined below) for the particular use case;

- The individual(s) that will be directly responsible for managing the data in question;
- The purpose for which the data is being requested;
- How the data will be used and why disclosures of Personally Identifiable Information and Student Data (defined below) are necessary to carry out that purpose;
- Duration for use of Data and deadline for destruction;
- Whether or not the use case requires data linking; and
- Information about relevant laws or guidelines to be followed when sharing or working with the data, including technical, physical and administrative safeguards that will be used to protect Personally Identifiable Information at rest and in transit.

This Agreement shall be used exclusively for those uses permitted under the Family Education Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), and any other pertinent federal or state statutes and regulations. This Agreement shall be governed by the Data Governance rules and policies for security and privacy of the Governor's Office of Information Technology and will comply with CDE's Information Security and Privacy Policy, dated February 2014.

All requirements for data management, handling and security listed herein shall apply equally to third party vendors performing services for the Parties to this Agreement.

III. Definitions

Data means the representation of facts as texts, numbers, graphics, images, sounds, or video that are captured, stored, and expressed as Data. Data includes Personally Identifiable Information and Student Data.

Data Breach means unauthorized or unintentional use, exposure, disclosure, or loss of Data, which includes Personally Identifiable Information.

Data Consumer means an individual who receives, analyzes and reports results of Data from the Data Provider.

Data Governance means the oversight of data quality, data management, data policies, business process management, and risk management surrounding the handling of Data, and includes a set of processes that ensures that important Data assets are formally managed throughout the Party's, department organization, or enterprise.

Data Governance Manager means the individual responsible for the implementation and oversight of the Party's data management goals, standards, practices, processes, and policies. Each Party's Data Governance Manager is authorized, after following approved internal Data Governance policies, to approve the sharing and release of that entity's Data to entities outside of that entity.

Data Owner means a person having the responsibility and authority for an entrusted data resource. The Data Owner plays a key role in internal Data Governance within the entity. The Data Owner takes ownership of the operational, technical, and informational management of the Data. The Data Owner knows how to use the Data, to whom it can be released and the appropriate conditions and regulations that govern the use of the Data.

Data Provider means the original collectors of the Data.

Decision Making using Data means any instance where analysis of Data and subsequent results are used to help make an educational, administrative, or other decision.

Demographics, refers to the *minimum* set of Data elements that uniquely define a particular person, e.g., name, address, date of birth.

Demographic Data Set means a set of demographics that uniquely define a particular person.

Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. Section 1232g, means the federal law that protects the privacy of students' personally identifiable information.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191 and regulations promulgated thereunder by the U.S. Department of Health and Corrections (the "HIPAA Regulations"), means the federal law that establishes privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals and other health care providers.

K-12 means school education levels ranging from Kindergarten to high school graduation.

Linked Data means the resultant data set after two or more entities' Data have been linked through the link system.

Longitudinal Analysis means an analysis of Data or a population over time.

Personally Identifiable Information (PII) includes, but is not limited to all Student Data that includes 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. Personally Identifiable Information includes student electronic email address, cell phone number or any other information that allows physical or on-line contact with a student, and includes student discipline or criminal records, juvenile dependency records, medical or health records, disabilities, socioeconomic information, political affiliations, religious information, text messages, IP address, documents, search activity, photos, voice recordings, food purchase or geolocation information.

Risk Assessment of Linked Data is a review conducted of the results of two or more pieces of data linked together to answer a specific educational question. The focus of the Risk Assessment is to determine the level of risk (related to a data breach) introduced by combining data. The individual data providers will participate in the Risk Assessment to help determine if the new data set may have unique regulations and conditions governing its release and use that were not present prior to combining the data. The System Steward and Data Providers will agree on and carry out any additional security or steps that are required as a result of the Risk Assessment to ensure the integrity of the Linked Data, up to and including the decision not to release the linked data.

Role-Based Access means a method of regulating access to computer or network resources based on the roles of individual users within an entity.

State Agency means each principal department within the executive branch, including each board, division, unit, office, or other subdivision within each department, each office or agency within the Governor's Office, each state-supported institution of higher education, and each local district junior college; except that State agency shall not include any department, agency, board, division, unit, office, or other subdivision of a department that does not collect unit records.

Statewide Longitudinal Data System (SLDS) means a federal grant program that provided funds to support the successful design, development, implementation, and expansion of the existing K-12 longitudinal data systems to include early learning, post-secondary and workforce data linking and analysis. SLDS grant funds were used to increase capability and opportunities for data analysis, but were not used to increase the data collected. CDE only conducts longitudinal analysis on data already existing in its warehouse or as a result of the linking of existing data with existing data from other entities.

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; and program participation information required by state or federal law.

System Steward means the entity responsible for combining two data sets from different sources, and managing the resultant data set. If a CDE data system is being used, then CDE is the System Steward. If another entity is doing the calculations or derivations, then that entity becomes the System Steward. The System Steward will ensure that all provided Data will be handled with care, following all applicable State and entity information security policies. Whether the resultant Data set is produced from a CDE system, or derived manually at another entity, all involved Data Owners will participate in validation and risk assessments as defined in this Agreement.

IV. Data Governance Plans

Both Parties agree to have in place a Data Governance plan with support and participation from across their organizations that detail the organization's policies and procedures to protect privacy and data security, including ongoing management of data collection, processing, storage, maintenance, use and destruction. Each Party has the right to conduct audits or other monitoring of the other Party's Data Governance policies, procedures, and systems.

If, through these monitoring activities, vulnerability is found, the breaching Party must take timely appropriate action to correct or mitigate any weaknesses discovered. The Requestor's current data security policies and procedures are not posted on an externally facing website but will be provided to CDE prior to the signature of this Agreement and annually thereafter and must include the minimum security policies and procedures set forth below:

1. Privacy and Security Policy
2. Privacy and Security Board
3. Management Oversight
4. Privacy and Security Officer
5. Sanctions for Violations
6. Reporting Potential Problems in Privacy and Security
7. Incident Response
8. Privacy and Security Training

9. Minimum Necessary Access
10. Password Management
11. Verification for Access to Sensitive Data
12. Transmitting Sensitive Information
13. Log-in Monitoring
14. Access Control
15. Workstation Security Configuration
16. Faxing
17. Device and Media Control
18. Computer Monitor Copier Printer Locations
19. Securing Materials with Identifiable Information
20. Encryption
21. Authorizations for Personal Health Information, if applicable
22. Data Privacy and Security
23. Permitted Uses and Disclosures of PHI, if applicable
24. HIPAA Status, if applicable
25. Business Associate Status, if applicable
26. Designating Sensitive Information
27. Risk Assessments
28. Information Risk Management
29. Change Control
30. Audit and Evaluation
31. Documentation Privacy and Security Protocol
32. Incident Response Mitigation

V. Access Restrictions

A. The Parties agree to implement and utilize Role-Based Access to ensure that only authorized individuals have access to Data.

B. The specific records to be released from CDE shall be subject to the consent of CDE's Data Governance Manager (or designated authority).

C. The specific records to be released from Requestor shall be subject to the consent of Requestor's Data Governance Manager (or designated authority as noted in the appendices).

VI. Re-Disclosure of Data

A. Requestor and Data Consumer may not further use or disclose Data without authorization from the Data Governance Manager (or designated authority) of the Data Provider, the Data Consumer may only further disclose data in an aggregate form that does not allow the identification of individuals, except where permitted in Appendix A. No re-disclosure of individual level data is allowed, unless specifically required by Colorado or Federal statute. If required by statute, the statute will be cited as well as all related information required by FERPA in the respective appendix/use case. The Data Consumer may only further disclose data in an aggregate form that does not allow the identification of individuals.

B. There shall be no disclosure of individual level data to government agencies outside of the state.

VII. Data Ownership

A. The Data Provider shall maintain ownership of the Data. The Data Consumer shall not retain any right, title or interest in any of the Data furnished by the Data Provider.
   1. The Data Provider maintains ownership of the Data in the case of third party vendors who may house agency Data off-site. The Data Consumer is required to have a written agreement with any third party vendor who receives or uses PII to ensure the vendor will not further use or disclose the Data. Data will not be provided to any third party without the specific written consent of CDE.

B. The Data Consumer maintains a stewardship role for the preservation and quality of the Data.

   1. The Data Consumer may use and disclose Data as permitted in this Agreement and only in a manner that does not violate state, or federal privacy regulations adopted by the Data Providing Agency. The Data Consumer may not sell or disclose the Data for any commercial purpose.

VIII. Data Security Requirements

A. The Data Provider shall ensure that no Personally Identifiable Information is transmitted through unsecured unencrypted connections.

B. All Data Consumers receiving PII from CDE must incorporate the following requirements:

   1. Strong access control must be in place. All data must be at a minimum protected with a complex password, workstations and other data processing devices must automatically lock when not in use, and must be manually locked when left

unattended. Passwords must be confidential and sharing of passwords is prohibited, must not be written down or stored in an insecure location, and periodically changed and not reused for a reasonable time period.

2. Unused and terminated user accounts must be disabled and/or deleted immediately; account inactivity must be periodically assessed for potential stale accounts.

3. Care must be exercised in inadvertently sharing data on display screens, during demonstrations or presentations, or when sharing screen shots for troubleshooting or other purposes.

4. Systems must be in place for logging and monitoring access and use of data.

5. At a minimum, annual intrusion penetration/vulnerability testing will be implemented.

6. Laptop/mobile device password locks and full disk/storage encryption are required.

7. Data at rest on central computing systems must be encrypted; any backup, backup media, removable media, tape or other copies must also be encrypted, and not used to transport data.

8. Mandatory annual security awareness training on how to handle PII is required.

9. Appropriate endpoint security anti-virus and anti-malware software must be installed and maintained on computers accessing or processing PII.

10. Transmitting data must occur via a secure method such as Secure File Transfer Protocol (SFTP) or comparable and never sent via email or transported on removable media.

11. Physical security in buildings housing PII, along with controlled physical access to buildings and/or data centers.

12. Ability to suppress small N-sizes for aggregated student data reports is required.

13. After prescribed use is concluded, data disposal policies must apply for cleaning up all data. This includes secure scrubbing and securely overwriting data from storage, or physically destroying the storage media.

14. Devices used to copy or scan hard copies of data must have encrypted storage and have storage devices appropriately scrubbed when equipment is retired. Hard copies

containing PII are discouraged and must be physically secured, not left unattended, and physically destroyed.

15. All data processing systems, servers, laptops, PCs, and mobile devices must be regularly scanned and have all security patches applied in a timely manner.

16. Data stored in cloud based systems must be protected in the same manner as local data, as described throughout this document. Use of free cloud based services is prohibited, and secondary encryption must be used as appropriate to protect data in cloud storage.

17. Cloud based hosting environments may not be located outside the state of Colorado.

18. Cloud environments, when employed, must be fully documented and open to CDE inspection and verification.

    a) Access to cloud based computing environments is only permitted via restricted access, by VPN or least privileged access lists, and never accessible directly via the Internet.

C. The Data Consumer agrees to abide by all applicable federal and State laws and regulations, including FERPA and others as specified in attached appendices.

D. The Data Consumer shall permit the Data Provider to investigate any report of a Security Breach or improper use of Data and to examine the Data Consumer's premises, records and practices. The Data Consumer agrees to abide by the resulting notification procedures outlined by the Data Provider in the event of a breach.

IX. System Steward Duties

A. The System Steward maintains a stewardship role for the preservation and quality of the Data.

B. The System Steward shall manage the source system, and ensure the integrity and safety of the Data at all times.

C. The System Steward shall follow all security requirements outlined in Section VIII or this agreement, to prevent use or disclosure of Data not authorized by either this agreement or the attached appendices.

D. The System Steward agrees to abide by all applicable state and federal laws and regulations, including FERPA, HIPAA and others as specified in attached appendices.

X. Release of Data to Data Consumer

If CDE or Data Consumer will combine the data with data from another source, the result could be a new data set with potentially unique regulations and conditions governing its use. If this occurs, the following applies:

A. Prior to sharing the new data set with Data Consumer, the System Steward will classify the linked data according to risk of data breach. This could include evaluating based on method of release, or on likelihood of identifying Personally Identifiable Information from the linked data (or violating other regulations that apply to the linked data).

B. Based on the above classification, if PII will be released, a full Risk Assessment shall be conducted prior to release. The following questions shall be asked:

1. Does use or disclosure of the new data set comply with FERPA?
2. Does the new data set meet the original request and can it be used in the way that the Data Consumer planned?
3. What conditions and/or regulations apply to the new data set?
4. Does usage of the new data set pose a high risk of breaching those regulations?
5. Have reasonable and appropriate steps been taken to reduce the risk of breach during the actual transfer of data to the Data Consumer?
6. How will the data be protected at rest and in transit?
7. Other questions may be added, as appropriate.

C. Results of the Risk Assessment shall be provided to Data Providers for review.

D. Based on the results of the Risk Assessment and recommendations from Data Providers, the System Steward shall apply additional constraints as necessary to the usage of the new data set. Options shall, at a minimum, include:

1. Require Data Consumer to destroy data after 6 months (or less if the risk is determined to be high), with accompanying proof of destruction submitted to System Steward;
2. The System Steward must follow-up after specified time period to review results of data usage by Data Consumer; and
3. Data Consumer must agree that no PII will be released to additional third parties.

Final agreement on additional constraints shall be documented in the Appendix, and signed by the Providers, the Requestors and System Steward as appropriate, **prior to** ***release of new data set.***

XI. Data Accuracy

The Data provided are the best and most complete documentation available. CDE and Requestor do not ensure 100% accuracy of all records and fields. Some data fields, including those that are not used, may contain incorrect or incomplete Data. CDE and Requestor will report any systematic problems with the Data identified in linked data sets to the Data Owner. Data that has been manipulated or re-processed by either CDE or Requestor is the responsibility of the user.

XII. Confidentiality

A. The Parties agree to protect Data and information according to acceptable standards and no less rigorously than they protect their own confidential information. PII will not be reported, disclosed, re-disclosed or made public.

B. All Data sharing shall be performed in accordance with the requirements of FERPA. FERPA Section 1232g(b)(1)(F) provides that education records and PII may be released without student or parental consent to "organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administrating predictive tests, administering student aid programs, and improving instruction, if such studies are conducted in such a manner as will not permit the personal identification of students and their parents by persons other than representatives of such organizations" [and other precautions are taken].

C. Additionally, CDE shall comply with any agency or program specific regulations outlined in C.R.S. Title 22 that governs the sharing of protected information.

D. All State Agencies and vendors agree to abide by all state and federal laws, rules and regulations, including FERPA regarding the Data specified in the appendices.

E. To the extent applicable, all Data sharing shall be performed in accordance with the requirements of HIPAA. HIPAA Section 164.514(a)-(c) provides that de-identified personal health information may be released without the individual's specific written permission. Additional provisions existing in C.F.R. Title 45, Parts 160, 162, and 164 shall be complied with as they apply to this agreement.

F. CDE and Requestor shall not disclose, release, reveal, show, sell, rent, lease, loan or otherwise grant access to educator or student PII and/or any Data derived or extracted, to any individual who does not need the Data to complete their work assignment as required by their job responsibilities within the scope of this Agreement. This includes reports,

written or oral presentations, written analysis, study articles or any similar documents containing Data.

XIII. Non-Financial Understanding

This Agreement is a non-financial understanding between CDE and Requestor. No financial obligation by or on behalf of either of the Parties is implied by a Party's signature at the end of this Agreement. The terms of any financial liability that arises from data processing activities carried out in support of the responsibilities covered herein must be negotiated separately and to the mutual satisfaction of the Parties. The legal authority for data sharing for specified purposes conveyed by this Agreement cannot be used to support a subsequent claim of implied agreement to financial obligation.

XIV. Data Retention

A. Data Consumers agree to safely maintain Data while conducting the research specified in the Agreement. All unnecessary records shall be purged at the earlier of the expiration of this Agreement or sooner if it has been determined there is no longer an educational purpose or research value. Records shall either be returned to the Data Provider or destroyed in a secure manner. Any additional data retention/destruction requirements unique to a particular use case will be described in detail in the relevant Appendix.

B. Any external party housing Data on behalf of one of the Parties must agree in writing to the same privacy and security standards, restrictions, and conditions set forth in this Agreement.

XV. Unauthorized Uses, Disclosures or Breaches

A. In the event a Data Breach occurs as a result of Data sharing, the Data Consumer shall be responsible for notifying the Data Provider and working with the respective entities' Data Governance Managers (or delegates as noted in the appropriate appendix) in contacting and informing the individual students, persons or entities who may have been affected by the Data Breach. Data Consumers may not contact individual students or entities prior to notification of the Data Provider.

B. The Requestor shall permit the Data Provider to investigate any such report and to examine the Data Consumer's premises, records and practices. The Requestor agrees to abide by the resulting notification procedures outlined by the Data Provider in the event of a breach.

C. Should a person not comply with this Agreement, he/she may be subject to disciplinary action, including, but not limited to, termination of access authorization.

D. Failure to comply with this Agreement may result in denial of access or any actions deemed "inappropriate dissemination of student or staff data". In the event of a Breach of Data, the Breaching party shall pay all the costs of remediating the Breach.

E. CDE and Requestor shall make a good faith effort to identify any use or disclosure of confidential Data not authorized by this Agreement.

F. If there are costs associated with notifying individuals whose PII has been compromised or any other damages resulting from the release of the Data, the compensating party shall depend on determined fault for the initial Data breach. If the Data Provider is responsible for the breach, the Data Provider shall compensate for communication and damages. If the Data Consumer is responsible for the breach, the Data Consumer shall compensate for communication and damages.

XVI. Survival

The respective rights and obligations of Parties shall survive the termination of this Agreement with respect to Data previously shared.

XVII. Data Requests

The Parties shall follow the agreed-upon Data governance rules and policies for security and privacy of the Governor's Office of Information and Technology. CDE and Requestor will hold Data Owners and Data Governance Managers accountable to ensure their Data is handled by the authorized individuals necessary to achieve the stated purposes, while still conforming to all regulations and security policies.

XVIII. Effective Date and Term

This Agreement shall take effect upon its signing by all Parties. This Agreement may be amended at any time by mutual agreement of all Parties. All Parties will conduct an independent review of this Agreement on an annual basis. This Agreement shall remain in effect until terminated by written notification from one Party to another.

XIX. Signatures

To further the collection and analysis of Colorado educational Data, CDE, represented by the Interim Commissioner of Education, and Requestor, represented by Stefani Shek agree to the cooperative sharing of Data between the Parties pursuant to the conditions set forth herein.

Signature: Katy Anthes *Date:* 6/21/16

Katy Anthes, Ph.D.

Interim Commissioner of Education

Colorado Department of Education

Signature: _____ *Date:* 6/21/16

Stefani Shek

Associate Director

Industrial Contracts Office

Stanford University

APPENDIX A – Business Use Case

Purpose

The Center for Research on Education Outcomes (CREDO) at Stanford University seeks an agreement with the Colorado Department of Education (CDE) to obtain longitudinally-linked student records, identified only through a scrambled unique ID, to support a research evaluation it plans to conduct in 2016. The research question to be explored is: "Do students in charter schools operated by Charter Management Organizations or other charter school networks fare better academically than students who attend independent charter schools or traditional public schools operated by districts?"

The aim of the research is to provide education leaders and policy makers with solid evidence about program and policy performance for their use in decision making. Since charter schools and Charter Management Organizations in particular are dynamic in size and effort, current assessment of whether and how they are effective can have immediate value in policy discussions.

System Steward

The System Steward for this use case is CDE.

Data Consumer

The Data Consumer for this use case is the Center for Research on Education Outcomes (CREDO) at Stanford University.

Data Provider

The Data Provider for this use case is CDE.

Request

This project requires the use of student-level data detailed in the table below to determine the impact of charter school attendance, school closure, and cyber-school attendance on student outcomes. This project may lead to a greater understanding of the impact(s) of charter school

attendance, school closure, and cyber-school attendance on student outcomes in Colorado and nationwide.

Output

We expect to produce a report of our research findings on the performance of Colorado's charter schools, both in Charter Management Organizations (CMOs) and networks, and those that operate on a stand-alone basis. CREDO's research analysis will be provided to CDE in order that CDE may be better informed about the impact of charter school policies on the advancement of students, in particular students who face educational challenges. Additional details about the planned analysis are presented below.

CREDO will post the report on the CREDO website and distribute it to partners in state education agencies and other interested stakeholders.

Participating Agencies

The **Colorado Department of Education** (CDE) will be sharing data with the **Center for Research on Education Outcomes** (CREDO).

Duration of Study

The study referenced in this appendix will end on December 21, 2017. The agreement will be reviewed, updated and approved on an annual basis. CDE may terminate this Agreement at any time, for its own convenience, for any reason, with written notice to the Requester. The Requester may terminate this Agreement for any reason, with 30 days written notice to the State.

Conditions under which data may and may not be linked and shared

For the purpose of the above business use case, the roles of Data Consumers shall be limited to the identified data consumers. CDE and Requestor may identify additional staff as Data Consumers in writing for review and consideration. Requestor includes as data consumers James Lynn Woodworth, William Snow, W. Payton Richardson, Yohannes Negassi, Chunping Han.

The role of Data Governance Manager for CDE is Marcia Bohannon for this agreement, and the role of Data Governance Manager for Requestor is William Snow.

Table of Required Data and Ownership:

Data Elements	Data Owner

Scrambled student identification number (from the state or district) that can be linked across years	N/A
• State achievement test scaled scores (Reading/ELA and Math for all students plus end of course exam scores for high school students) for all available years starting with the 2004-2005 school year. • Performance levels, or achievement or proficiency categories, usually given in the following categories (for each subject): below basic, basic, proficient, advanced and additional categories such as far below basic or above advanced, if applicable • School identification number for each school the student attended on the testing date each year • Race/Ethnicity • Gender • Lunch Status or Other Measure of Low Income Status • Special Education Status • English Proficiency • Grade Level • Full student enrollment files for each year we are given, including date entered, date exited, days of possible attendance, days attended and school attended (ID & name of school). • Graduation flag (high school students only) • Course completion records (high school students (only) • List of charter schools by district and school ID (if applicable). • Grade level means and standard deviations for the state reading and math tests for each year we are given (aka technical report). • Conditional standard error of measurement tables for each grade, year and subject test, i.e., standard error for each individual scaled or raw score. • Cut scores for proficiency bands. • Unique school identifier (or unique district and school ID combination) that is linkable to federally published school data for your state. • Teacher-student linkage; alternative if not available: individual teacher data file with all available teacher demographics and school/grade teaching assignment	Joyce Zurkowski

Research Questions

The Center for Research on Education Outcomes (CREDO), a nonpartisan policy and program evaluation group at Stanford University, is currently conducting research to learn more about the effectiveness of charter schools and other public schools. One of CREDO's aims is to evaluate the impact of charter school attendance on student academic progress in relation to the institutional affiliation of charter schools with either Charter Management Organizations (CMOs) or other charter school networks. A second aim of the study is to examine the trends in performance of charter schools as a function of characteristics of the overall environment for

charter schools, the closure of charter schools for poor performance and the rates of growth over time.

Research Methodology

There are two different kinds of "combining" that CREDO will to do with the data provided by CDE.

First, to every student record in every year, CREDO will attach a profile of the school the student attends that year. The school data is aggregated across all the students in a school in a given year and comes from CREDO's national school database, which is curated from publicly available sources. The school profile data contains no PII and describes only the overall demographic character of the school, the grades served and school and grade enrollment.

Second, CREDO will use student-level data from CDE and similar data from approximately 30 other states to study the research questions on a broad scale. CREDO's research approach is structured as a "twins" study – one student in a charter school is compared to a counterfactual in a different school. Both students are drawn from the same locality, so the progress of students in Colorado charter schools are only compared to students in other Colorado schools. CREDO combines the datasets from multiple states to create multi-state measures of charter school performance as a national picture.

CREDO contends that a true measure of school effectiveness is the amount of progress or growth that a student experiences each year when enrolled in a school. Cohort- or school-level measures of achievement are sullied by the moves, adds and progression through the grades, yielding a year to year estimate that can reflect substantially different students, and therefore is ineffective as a measure of school impact.

CREDO will use growth in standardized test scores as the measure of student learning. By differencing the standardized scores in successive years, an incremental measure of progress can be obtained. Because students are followed longitudinally, their background characteristics remain largely constant, thereby producing an unclouded measure of learning gains. These measures of standardized test score growth, referred to a z-score growth, form the outcome of interest in many of the questions about charter school impacts that the proposed study will seek to answer.

The study will analyze the rate of learning progress in charter school students compared to their virtual twins. The model will provide statistical controls for personal and schooling factors as well as eligibility for program participation based on poverty, language or special education needs. The control variables will illuminate whether overall performance of the samples varies systematically by student characteristics other than school type.

The VCR methodology permits this study to advance the insights of charter school impacts for students who spend one or more years enrolled in charter schools. For each charter school, the VCR method executes a matching procedure for each charter school student, drawing from students in district schools that have lost students to that specific charter. The match is based on demographic characteristics, eligibility for lunch subsidies, English Learner status, Special Education status and, importantly, prior achievement. Up to seven matched students from the pool of district schools (known as the "feeder" pool) are chosen; their progress is then averaged to provide the counterfactual for the charter student. This design creates a matched pair of students – one whose academic year is spent in charter schools and one who is educated that same year in district schools – and uses the same subject test in the same year in the same state to test the performance of charter schooling on student academic gains.

The results of the econometric models will be refined by looking at interaction effects. In these models, the learning gains in charter schools will be studied to see if they differ by student-level characteristics, such as race, gender, grade, baseline starting scores or program eligibility. In addition, CREDO will examine whether results differ by the number of successive years students attend charter schools. The aim of these models is to see if, beyond the average charter effect obtained in the model described above, there are subsets of students for which charter school attendance produces significantly stronger or weaker results.

Requestor Processes

The Requester, representing all members of the research team supporting the aforementioned research study, shall:

- Use student records appropriately, only for authorized purposes, and never for commercial purposes in accordance with federal and state law and as specified in this Agreement, including the confidentiality, transparency and data security provisions contained herein;

- Destroy student records that have been provided from the State pursuant to time limitations defined in the Agreement and, if requested, provide certification that such records have been destroyed;

- Prior to public dissemination/release, if requested in writing by the State at least thirty (30) days before scheduled release, and subject to the following, provide reports generated as a result of using student records received from State to permit the State to verify that the intended purpose has been adhered to and that the publication contains no confidential student information;

- CDE reserves the right to receive a final copy of the research report and post that report on

CDE's public facing website;

- The State will ensure that access to the report is permitted on a need-to-know basis only for this verification purpose and will protect the report from public dissemination or release; and
- Understand that deliberate or accidental misuse of student records may result in one or more of the following: loss of access, dismissal from work, legal action including prosecution under the scope of any applicable federal and state laws.

The Requester shall not:

- Share student records with any individuals or third parties not included in the Agreement;
- Publish reports with a cell size of less than 16. (Reports must mask these cells so that results are not revealed.)

Regulations that Apply

- FERPA (34 CFR Part 99, section 99.3)

Signatures

To further the collection and analysis of Colorado educational Data, CDE, represented by the Interim Commissioner of Education, and Requestor, represented by Stephanie Shek agree to the cooperative sharing of Data between the Parties pursuant to the conditions set forth herein.

Signature: Katy Anthes *Date:* 6/21/16

Katy Anthes, Ph.D.

Interim Commissioner of Education

Colorado Department of Education

Signature: _____ *Date:* 6/21/16

Stefani Shek

Associate Director

Industrial Contracts Office

Stanford University