GDAB Annual Report 2017

COLORADO

Governor's Office of Information Technology

Serving people serving Colorado

COLORADO
Governor's Office of Information Technology
Serving people serving Colorado

January 18, 2018

Dear Secretary Nallapati,

It is my pleasure to deliver the 2017 Government Data Advisory Board (GDAB) Annual Report in accordance with C.R.S. 24-37.5-701 et seq.

This report reflects ongoing work by the GDAB to improve data governance and interagency data sharing. This particular work was identified as important for data sharing when the GDAB began meeting again in 2016. It has relied on significant contributions by GDAB members and has created momentum for continued activities that will expedite data sharing while enhancing data privacy and security. Specifically, the GDAB has:

- Developed a commonly accepted and understood vocabulary for data sharing and governance. This lexicon provides a standard set of definitions for use in data sharing agreements across the state enterprise, and it will be incorporated into OIT processes and data sharing agreements going forward.

- Defined a standard framework for data governance. Standardized data governance will facilitate data sharing and improve the security and privacy profile for the state's data assets. The data governance framework developed by the GDAB is based on a maturity model approach that provides flexibility for state agencies. Rather than imposing a mandatory, monolithic structure for data governance, the maturity model allows agencies to assess their level of maturity and identify specific steps to increase their data governance maturity based on available resources and organizational structure.

- Supported development of a common framework for data sharing agreements. Health agencies in the state have developed a common data sharing agreement, and the GDAB followed this work and expects to adapt this for broader applicability in 2018.

In addition, the GDAB received updates and provided feedback on data-related issues such as amendments to the Open Records Act and the Evaluation and Action Lab at the University of Denver. The annual report also sets out the work agenda for the GDAB in 2018. This includes developing a toolkit and protocol to expedite data sharing among agencies.

I look forward to any comments you may have about this work. Of course, if you have any questions or concerns, please do not hesitate to contact me.

Best regards,

Jon Gottsegen
Chief Data Officer

Introduction

The State of Colorado has recognized that greater efficiencies and innovations in state government will be achieved through improving data sharing processes and procedures. While there are several advanced data management programs and data sharing or integration efforts among state agencies, data sharing between state agencies continues to require labor intensive execution of data sharing agreements and manual transfer of data using a wide variety of tools adopted by state agencies independently. Additionally, the lack of a standard data governance framework across the state enterprise results in data being managed differently among state agencies. This hinders data sharing, as an agency that is sharing data may not have a common reference with the requesting agency for how the shared data may be handled.

More efficient and effective data sharing and integration will make data available for sophisticated analyses of policy and program effectiveness across state programs. With more standardized approaches to governing and sharing data across the enterprise, the sharing of data will also be better governed, thereby protecting the data and the value invested in those data by the state.

Improving data sharing, integration and governance has been the focus of the state's Government Data Advisory Board (GDAB or the "Board"). The Colorado General Assembly recognized this need for more effective sharing and governance of data when it created the GDAB in 2009 specifically to advise the State Chief Information Officer (State CIO) on activities and policies necessary for developing an interdepartmental data protocol. This protocol should facilitate information sharing across agencies and assist in determining the effectiveness of state policies related to data sharing, governance and distribution to the public. The interdepartmental data protocol and GDAB are codified in C.R.S. 24-37.5- 701 et seq. The Board is managed and chaired by the Governor's Office of Information Technology (OIT).

The Board was preceded by a Data Protocol Development Council (Council), also created by statute to provide guidance, policies, and procedures for implementing a data sharing architecture across the state enterprise, and driven by the need to use data across state agencies to analyze the effectiveness of state policies and inform strategy for the use of state resources. Before it sunset, the Council recommended establishing a formal governing board, which ultimately became the GDAB, to advise on enterprise policies, directions and priorities for data governance and management across agencies. While the GDAB's work followed the Council's focus on unit records (i.e., records pertaining to individuals within the state), it now provides recommendations on records of any type. Nonetheless, unit records will continue to be a priority for the Board due to the privacy and compliance related issues surrounding them.

Vision

The Board's vision is to increase the effectiveness and efficiency of government services by promoting greater collaboration, innovation, and agility in government operations through more regular data sharing between state agencies and political subdivisions and more seamless, efficient, and strategic exchange of core data sets while protecting privacy and security of data.

The Board has the following cross-departmental responsibilities:

- Advise the state's Chief Information Officer (CIO) on the development, maintenance, and implementation of the data sharing protocol;
- Advise on the best practices for sharing and protecting citizen data;
- Review, advise, and provide input into the strategic plan for improving data governance;
- Advise on compliance, privacy, and security data requirements;
- Advise on internal and external data policies and procedures;
- Advise on financial and budgetary components required for implementation; and
- Specifically recommend education data sharing and management strategies.

Goals

The Board's mission is to facilitate information sharing across agencies and assist in formulating and determining the effectiveness of state policies. The Board's specific goals are as follows:

Goal 1: Develop recommendations for enterprise data sharing, integration, and consolidation, particularly in the area of data sharing agreements.

Goal 2: Recommend policies and procedures for managing data and resolving data sharing or data management conflicts.

Goal 3: Identify areas to reduce operational costs and complexity.

Goal 4: Provide recommendations to improve data privacy, regulatory compliance, and access management.

Goal 5: Establish an enterprise data governance framework and provide recommendations and best practices to improve data governance within the state enterprise.

Goal 6: Identify change management opportunities (e.g., service delivery, process improvement, organizational re-alignment) to enhance data governance and data sharing.

Goal 7: Provide feedback and guidance on an open data strategy for the state.

2017 Work Activities

The Board met monthly through the 2017 calendar year. In addition, the Board formed two working groups to work on the standard data governance framework and the standard data lexicon (i.e., dictionary). The specific meeting dates are listed in Appendix A.

Membership

State statute (C.R.S. 24-37.5- 703) specifies the state and local agencies that must be represented in the Board's membership, while also allowing the governor to include representatives designated by the executive directors of additional agencies. Statute also allows the secretary of state, attorney general, state treasurer, and the chief justice of the supreme court to select a member from his or her department. Currently the Board membership includes the departments of:

- Corrections
- Education
- Health Care Policy and Financing
- Higher Education
- Human Services
- Labor and Employment
- Natural Resources
- Public Health and Environment
- Public Safety
- Revenue
- State
- Transportation
- Office of eHealth Innovation

Local representation includes:

- Douglas County
- Jefferson County School District
- Littleton School Board

The state Chief Data Officer (CDO) serves as an ex officio member and chair of the Board. The specific members representing these agencies and statutory language directing the Board's membership are included in Appendix B. In addition to these official members, there has been participation from the Governor's Policy Office, OIT's Office of Information Security as well as other staff from within OIT.

Work Agenda

In 2016, the Board identified several objectives to improve sharing and governance of data in the state. These objectives were identified to overcome organizational obstacles to data sharing and to realize opportunities for improved management of data across the state enterprise. Current pain points or challenges in data sharing can be categorized into:

- Statutory or programmatic restrictions
- Data governance practices (or lack thereof)
- Technological needs
- Data sharing agreements and policies
- Relationships between and within agencies

Benefits or drivers for improving data sharing in the state fall into the following categories:

- Statutory or legal drivers
- Improved data governance
- Interagency relationships and data interoperability benefits
- Technology improvements and innovation
- Strategic and organizational benefits

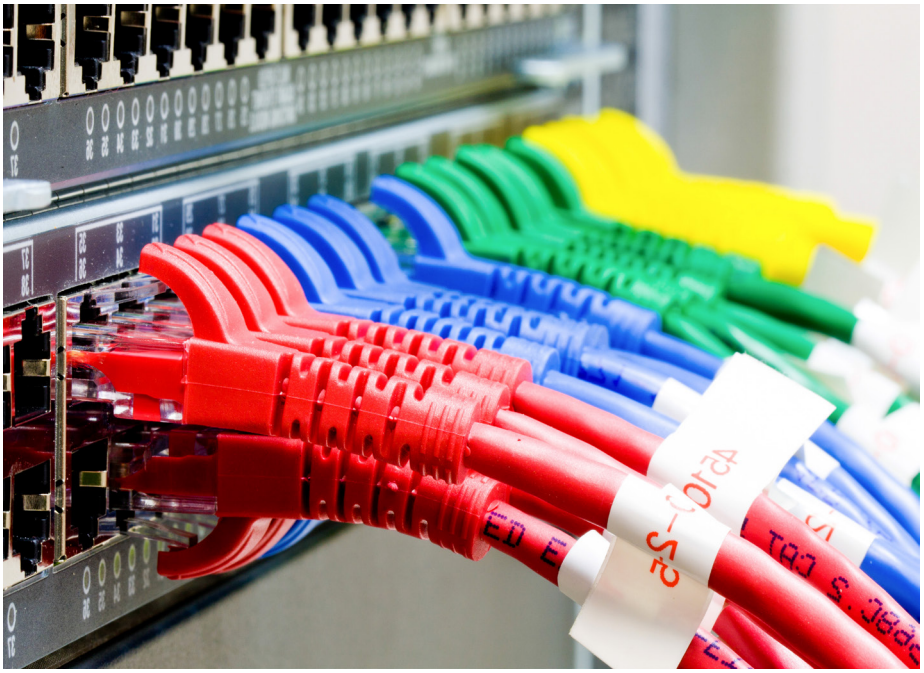
The Board's first product was a document titled *Why should Colorado develop an interdepartmental protocol?* that describes the obstacles to and drivers for improved data sharing and governance in greater detail. This led to a work agenda to improve the data sharing and governance environment in the state, and this work agenda continued into 2017. Specifically the agenda for 2017 and the resulting products from the GDAB included the following:

1. Data Sharing Lexicon:

The GDAB identified the need for a common language or lexicon when agencies talk about data sharing or data governance-related issues. Up to now, data sharing agreements from different agencies had their own definitions with varying terms or common terms that are used in different ways. This can lead to confusion or misunderstandings between the parties involved. Consequently, the GDAB set out to agree on a standard set of terms and definitions that can be referred to across state agencies when considering data sharing agreements or conditions for data sharing as well as discussing other issues related to data governance or management. After first simply agreeing on a discrete set of terms, and therefore specific concepts, that are salient when sharing data or discussing data management or data governance issues, the GDAB then agreed on definitions for these terms. This agreed on lexicon is included in Appendix C. To promote the use of this lexicion, the Board members desired to first socialize it in a manner non-intrusive to current agency activities.

Accordingly, the next steps will be to include it in data sharing agreements, integrate it into OIT's glossary, and promote its use by the system engineers and business analysts as they develop projects within OIT. Other opportunities for institutionalizing this terminology will be pursued as they arise as well.

2. Data Sharing Agreement:



The need for a common data sharing agreement structure was identified to overcome redundant efforts executing data sharing agreements when agencies share new data sets or data that has been altered. This has been a concern for state agencies for several years, and previous attempts were made by the GDAB to develop common data sharing agreements. Currently, when state agencies try to share sensitive data (sometimes any data), most agencies require a data sharing agreement that establishes the expectations for responsibilities and liabilities for the data. Often, each time data is shared, and consequently with each iteration of the agreement, a new agreement must be executed and approved by the agencies' legal staff and executive even if the new data being shared is very similar to previous data either in its content or use by the receiving entity. An agreement that remains somewhat constant and standard and that can be approved once will avoid these costly, repetitive efforts.

Recently state agencies concerned with health issues and health data (i.e., the Colorado Departments of Health Care Policy and Financing, Human Services, and Public Health and Environment) along with the Governor's Health IT Coordinator, have made significant progress on creating a standard data sharing agreement they can each sign. This agreement has been drafted and agreed on by the contracts teams and data experts within each agency and is now being reviewed for signature by their respective Executive Director's Offices. GDAB members followed this effort closely and used the Board meetings to establish how common approaches to data governance and standards can support such common agreements. While there was some ambition to consider such an enterprise-wide agreement during 2017, the development of this agreement among the health agencies has been a lengthy process and has taken the better part of the year. Expanding this agreement to other agencies will, in fact, require one or more years of work. In addition, the GDAB has recommended that such an enterprise-wide agreement be reviewed by the Office of the Attorney General to ensure it has proper legal standing. This agreement is included in Appendix D.

3. Data Governance:

An enterprise approach to data governance is necessary to preserve the value, security, and integrity of data assets in the state. The issue of varying data governance policies and procedures across state agencies puts the state's data at risk and does not preserve or yield full advantage of the state's data assets. It potentially also leads to redundant data management and confusion about which data should be used for what purpose.

The GDAB reviewed several data governance maturity rubrics and adapted them into one that fits Colorado's needs. It is important to recognize that different agencies have differing levels of capacity or capability for data governance, so the GDAB set out to present a "sliding scale" of governance maturity so an agency may identify where along that scale it currently is positioned and how it can advance its maturity in data governance. Accordingly, the GDAB developed a data governance framework in the form of a maturity model for data governance, and it developed a matrix articulating the various levels of maturity based on a general application of the five maturity levels from the Capability Maturity Model Integration (CMMI). Further, the GDAB recognized that before improvements could be made, they needed to first identify what level of governance is already in place within the agencies. The Board approved a data governance maturity self-assessment tool which presents a set of questions, with examples of how these questions may be answered, to assign a specific maturity level for various components of data governance. It provides an in-depth depiction of where an agency may improve its data governance and allows the agency to make informed choices regarding specific steps to enrich it. This framework is available here. [https://goo.gl/pW8jTg]

4. Open Data:

While Colorado has been committed to opening state data for public access, there has never been a concise, thorough strategy for open data in the state. Consequently a strategy that elucidates what constitutes open data, how those data will be published, and how public engagement with those data will be expanded is still necessary.

Colorado has expanded the number of data sets available on the state's open data portal, the Colorado Information Marketplace at data.colorado.gov - or CIM, as it is more commony known. Currently the number of data sets available on CIM is 980, and is the result of the partnership with the Secretary of State's Office through their GoCode Colorado effort and efforts among OIT staff. The GDAB and OIT are reviewing t he functional requirements for an open data platform and will be evaluating whether a different software platform will meet the state's needs more effectively. The rubric for this review has been developed and the next step is the actual assessment of alternative options.

5. Data Sharing Policy:

An interagency data protocol implies a comprehensive program that includes many of the efforts described in this report, such as policies and procedures for data sharing, standards and practices for data governance, and potentially policies and recommendations for appropriate charges for data. There is a need for a clear policy regarding data sharing in the state that outlines data that should be shared by default, appropriate protections for sharing other data, and means for overcoming obstacles for sharing these data. The concept of sharing by default, when appropriate and with appropriate controls, is important in establishing the principle of data sharing as contrary to lack of data sharing simply due to issues such as convenience. An example of where this gap in data sharing was evident and impactful, and where a sharing by default policy would have improved information use by the state in a critical time, was after the Front Range floods in 2013. At that time, data were shared based on the sometimes ad hoc opinions of individuals maintaining the data at the time. This hindered the information used in response to the floods. The consideration of a policy raises the question of what authority the Board has and how such a policy may be enforced. OIT has authority to set information technology (IT) policies, but the Board expressed that agencies are more likely to adhere to recommendations and best practices than mandates, and that it would be more palatable to agencies, if such a policy were first socialized as a recommended procedure.

In 2017, the GDAB did not develop or consider a statewide data sharing policy, but the lack of a standard, statewide policy has become a significant concern of the Office of the Governor. Several activities within the Offices of the Governor and Lt. Governor are pointing to more explicit policy or statutory language for improved data sharing. Representatives from those offices have participated in the GDAB meetings and have used GDAB discussions to inform their considerations and otentially guide future data sharing efforts.

In addition to these objectives and deliverables, the GDAB reviewed other issues that arose during the year and helped state agencies respond. These include:

- Amendments to the Colorado Open Records Act (CORA) - Senate Bill 17-040 proposed several amendments to the existing CORA language to mandate more openness of data. These amendments require agencies to respond to requests for structured or “searchable” data by delivering these data in a structured and/or searchable form. A member of the Attorney General’s Office (AGO) discussed these amendments with the GDAB. The AGO is developing clarification of these amendments for state agencies and invited input from the GDAB on which issues or questions they should address or clarify.

- Governance, Risk, and Compliance tool - This tool is being used by the Office of Information Security to manage requirements and information related to compliance audits for protected information. The requirements can be specified for different types of protections and then associated with particular data sets or agencies that maintain such data and that may be subject to associated audits. This allows the state to be proactive in ensuring that the requirements are met and that data are protected adequately and consistently across the state.

- University of Denver Colorado Evaluation and Action Lab - This lab has been funded by the Arnold Foundation and supported by the Office of Lt. Governor to perform innovative, cross-agency analyses on the effectiveness of state policies or strategies. These analyses will look at what aspects of programs are more or less effective than others and what leads to this effectiveness, rather than simply whether a program is working or not. The analyses will cross agency responsibilities because the lab will look at the overall outcomes of these programs.

- University of Pennsylvania Actionable Information for Social Policy technical assistance grant - Colorado is included in a cohort of state and local entities to receive this assistance from the University of Pennsylvania. The assistance is directed at promoting “integrated data systems,” and their focus is primarily on the organizational issues in data sharing. This overlaps well with several inter-agency projects requiring data sharing.

Agenda for 2018

Based on the outstanding objectives from 2017 and the pressing needs for ongoing improvements to the data sharing and availability environment in the state, the GDAB will work on the following items in 2018:

- ***Data Governance*** - Continue to test and refine the data governance maturity framework and promote it to all state agencies, assisting them where requested in applying the self assessment tool to their agency data landscape.

- ***Data Sharing Agreement*** - Leverage the work done by health agencies to expand the applicability of the standard agreement language to other agencies. Ultimately, the ideal structure would be to make this a multilateral agreement that is signed by multiple agencies before new data sharing requests arise.

- ***Tactical Issues Related to Data Sharing*** - In an effort to make questions and solutions related to data sharing more concrete, the GDAB is embarking on identifying agencies' specific data sharing requirements (i.e., specific data requested from other agencies). With this knowledge, the GDAB representatives can address the specific issues around these data and then generalize broader solutions across the state enterprise.

- ***Data Sharing Toolkit*** - To expedite data sharing and avoid creating processes and procedures on an ad hoc basis for each data sharing request or use case, the GDAB has suggested creating a data sharing checklist (e.g., ensuring data ownership and stewardship are clear before passing data onto other agencies or receiving data from other agencies). This can develop into a toolkit for data sharing that agencies can utilize to facilitate the data sharing process from initial request to transfer of data and continuing governance of the data sharing agreement.

- ***Data Sharing Strategy*** - A long-term strategy and plan for sharing, management, and governance of data should be in place and is part of the responsibilities of the state CDO. The CDO will develop this plan and obtain feedback from the GDAB during the year.

In addition, the GDAB discussed the following possible ongoing roles or activities:

- Support technology initiatives related to data, such as the enterprise service bus (ESB). This may take the form of helping to shape the initiatives, communicating how state agencies may use or support the initiatives, or communicating these initiatives back to the agencies.

- Document use cases for sharing. The state needs to demonstrate the powerful business cases for and benefits of data sharing to generate sufficient momentum and support for the work that will be required.

- Promote data governance and other efforts beyond the IT or business technology groups. This will require GDAB membership to actively engage in this effort.

- Document data sharing efforts currently underway, issues encountered by these efforts, and the solutions they have developed. Data sharing is happening now, in some places more successfully than others. The state needs to support those efforts, learn from them, and ensure they are consistently protecting the privacy of Colorado's residents and businesses.

Appendix A - 2017 Government Data Advisory Board Meeting Dates

- January 18
- February 15
- March 15
- April 13
- May 17
- June 21
- July 26
- August 16
- September 20
- October 18
- November 15
- December 20

Appendix B - Government Data Advisory Board Membership

The following individuals have been approved as members of the GDAB:

- Marcia Bohannon, Chief Information Officer, Colorado Department of Education
- Jeremy Felker, Executive Director, Student Data Privacy and Reporting, Jefferson County Public Schools
- Tobin Follenweider, Chief Operating and Performance Officer, Colorado Department of Natural Resources
- Jonathan Gottsegen, Chief Data Officer, Governor's Office of Information Technology
- Neil Hagenbrok, Director of Business Technology, Colorado Department of Labor and Employment
- Mike Hardin, Director - Business and Licensing, Office of the Secretary of State
- Steve Norman, Director of Records Management, Colorado Department of Revenue
- Carrie Paykoc, State Health IT Coordinator, Governor's Office of eHealth Innovation
- Erik Sabina, Data Branch Manager, Colorado Department of Transportation
- Jack Reed, Statistical Analyst, Colorado Department of Public Safety
- Erik Sabina, Data Branch Manager, Colorado Department of Transportation
- Parrish Steinbrecher, Health Information Office Deputy Director, Colorado Department of Health Care Policy and Finance
- Jim Stephens, Littleton School Board
- John Thompson, Data Services Manager, Douglas County
- Michael Vente, Research and Information Policy Officer, Colorado Department of Higher Education
- Rick Vynke, Associate Director - Office of Planning and Analysis, Colorado Department of Corrections
- Chris Wells, Director of eHealth & Data, Colorado Department of Public Health and Environment
- Herb Wilson, Director of Technology, Colorado Department of Human Services (recently transferred to OIT and will be replaced)

Appendix C - Data Lexicon Approved by the Government Data Advisory Board

Term	Accepted Definition
Assurance	Activities designed to reach a measure of confidence. Assurance is different from audit, which is more concerned with compliance to formal standards or requirements.
Confidentiality	The preservation of authorized restrictions on information access and disclosure, including the means for protecting personal privacy and proprietary information.
Data	The representation of facts as texts, numbers, graphics, images, sounds, or video. Facts are captured, stored, and expressed as data.
Data Governance	The oversight of data quality, data management, data sharing and access policies, business process management, and risk management surrounding the handling of data, and includes a set of processes that ensures that data assets are formally managed throughout the state agency, department organization, or enterprise.
Data Minimization	The act of limiting the collection of personally identifiable information to the least amount of information required to complete a particular transaction or meet a business need or requirement.
Data Privacy	The governance of personally identifiable, confidential, and other sensitive information to ensure information, digital or otherwise, is being collected, shared, used and disposed in appropriate ways.
Data Redisclosure	The act of sharing or releasing information that was received from a data owner or provider and included in data recipient's data.
Data Provider	The agency, department or organization that is providing the data to be shared. This may or may not be the same group as the data owner.
Data Sharing	The act of transferring data or authorizing access to data from the data owner or provider to the data consumer or recipient.
Data Steward(s)	The data steward takes ownership of the operational, technical, and informational management of the data according to policies and procedures defined by the data owner or data provider.
Data Stewardship	The practice of managing data and providing users access to that data. Processes will be based on clear, inclusive, and well-documented data architecture.
Interdepartmental Data Protocol	File sharing policies, processes, and procedures that permits the merging of data for the purposes of policy analysis and determination of program

	effectiveness.
Integrity	The prevention of improper information modification or destruction and ensuring information nonrepudiation and authenticity.
Linked Data	The resultant data set after two or more agencies' data has been combined. Once a data set is linked, the linking organization becomes the data owner and is responsible for following all rules and regulations regarding the security and privacy of the linked data set.
Metadata	Metadata is "data about data." It includes data associated with either an information system or an information object, for purposes of description, governance such as identification of data owners and data stewards, legal and confidentiality requirements, technical functionality and security, use and usage, and preservation.
Protected Data	Data that is subject to one or more restrictions on its dissemination based on state statute or rule or federal law and explicitly restricted from disclosure under the Colorado Open Records Act.
Provenance	The description of the origins and evolution of data and its movement between systems.
Role-Based Access	A method of regulating access based on the roles or positions of individual users within a state agency, department organization, or enterprise.
Sensitive Data	Any information where the loss, misuse, unauthorized access to or modification of which could adversely affect the interest or the conduct of information systems or agency business activity, or the privacy to which individuals are entitled.
Unauthorized Use	An act where an unauthorized user accesses protected or sensitive or "state Confidential" data, or when an authorized user uses or releases protected, sensitive or confidential data in a method that which is not within the scope of its permissible use.

Appendix D - STATE OF COLORADO INTERAGENCY DATA SHARING AGREEMENT

SIGNATURE AND COVER PAGE

State Agency Colorado Department of Public Health and Environment	**Contract Number** 105711
State Agency Colorado Department of Health Care Policy and Financing	**Contract Performance Beginning Date** The Effective Date
Contract Description: This Contract governs and memorializes the sharing of data between the Colorado Department of Public Health and Environment, and the Colorado Department of Health Care Policy and Financing.	

THE PARTIES HERETO HAVE EXECUTED THIS CONTRACT

Each person signing this Contract represents and warrants that he or she is duly authorized to execute this Contract and to bind the Party authorizing his or her signature.

STATE OF COLORADO John W. Hickenlooper, Governor Colorado Department of Public Health and Environment Executive Director _____ By: Signatory Date: _____	**STATE OF COLORADO** John W. Hickenlooper, Governor Colorado Department of Health Care Policy and Financing Executive Director _____ By: Signatory Date: _____
STATE CONTROLLER **Robert Jaros, CPA, MBA, JD** _____ By: Signatory Date: _____	**LEGAL REVIEW** Cynthia H. Coffman, Attorney General By:_____ Assistant Attorney General Date: _____

1. PARTIES

This Interagency Data Sharing Agreement (hereinafter called "Agreement") is entered into by and between the Colorado Department of Public Health and Environment at 4300 Cherry Creek Drive South, Denver, Colorado 80246, (hereinafter called "CDPHE"), and the Colorado Department of Health Care Policy and Financing at 1570 Grant Street, Denver, Colorado 80203, (hereinafter called "HCPF"), who may collectively be called the "Parties" and individually a "Party", both of which are agencies of the STATE OF COLORADO, hereinafter called the "State".

2. EFFECTIVE DATE

This Agreement shall be effective once it is approved and signed by the Executive Director, or an authorized delegate, from each Party.

3. RECITALS

A. Authority, Appropriation, and Approval

The Parties each possess the authority to enter into this Agreement. Required approvals, clearance and coordination have been accomplished from and with appropriate Departments.

B. Consideration

The Parties acknowledge that the mutual promises and covenants contained herein and other good and valuable consideration are sufficient and adequate to support this Agreement.

C. Purpose

The purposes of this Agreement are to lay out minimum standards for data management, privacy and security, condense records of all existing and future sharing of data between the Parties into a single document, and to assist in the tracking of all shared data in order to ensure that sufficient privacy and security controls are used to protect shared data.

D. Scope

This Agreement shall cover all data sharing activities between the Parties to the extent applicable.

This Agreement shall be used exclusively for the purposes of describing the Data being shared between the Parties to the extent applicable. All Data shall be shared with the intention of using the Data for decision making, publishing, reporting, longitudinal analysis, research, policy making, or any other use permitted by the applicable governing authorities.

4. TERMINOLOGY

Terms shall be construed and interpreted as described in Exhibit A, Definitions unless specifically redefined in another section of this Agreement, or in any attached document. All other terms shall be given their plain meaning.

5. TERM

The Parties respective performances under this Agreement shall commence on the Effective Date. This Agreement shall continue in perpetuity, unless sooner terminated by either Party. Either Party may terminate this Agreement by giving the other Party at least 30 days prior written notice setting forth the date of termination.

6. COMPENSATION

No Party shall provide compensation to any other party under this Agreement. The Parties agree that in the event that compensation should become necessary between the Parties, the Parties will enter into a separate Agreement to determine that compensation.

7. PRIMARY CONTACTS

Each Party shall designate a primary contact who shall serve as the primary contact for that Party. The Primary Contact shall ensure that all amendment and other procedures for the management of this contract are followed.

8. DISPUTES

In the event of disputes concerning performance hereunder or otherwise related to this Agreement, the Parties shall attempt to resolve them at the divisional level. If this fails, disputes shall be referred to senior Departmental management staff designated by each Party. If this fails, the executive director of each Party shall meet and attempt resolution.

If there is a conflict between provisions in the Parties' Data Governance Plans, the Parties will work together to identify the most appropriate provision to follow, and shall include the agreement in the Appendices, or wherever is appropriate. If the Parties cannot agree, then the Provider's provisions will apply.

9. REVIEW AND AMENDMENT

A. Amendment

i. Except as otherwise provided in this Agreement, any modification to the terms of this Agreement shall only be effective if agreed to in a formal amendment to this Agreement, and is properly executed and approved by the Executive Directors or delegates of both Departments.

B. Appendix Addition and Amendment

i. Appendices may be added to this data Agreement only through a formal amendment to this Agreement.

ii. Appendices may be modified without full amendment of the entire Agreement via mutual Agreement in writing between the program contacts if the changes would not increase the protections on the data or increase the amount of data being transferred. This includes, but is not limited to the following specific cases.

a. Altering the purpose of the project

b. Altering the contact persons

c. Altering the term for sharing and/or retention of the Data

d. Altering the file format

e. A decrease in the data elements.

f. Altering the period of time the Data covers

g. Altering how often Data will be updated

h. Additional privacy and security controls.

i. Altering the persons and positions whom will be authorized to have access to the Protected Data.

iii. Any other modification to an Appendix may be done using an Option Letter originating from the Party providing the Data. The Option Letter shall be substantially similar in form to Exhibit C, Sample Option Letter, and shall include an updated version of the Appendix or Appendices that will be changed.

iv. Any modification shall not reduce the protection of the data below the minimum standards laid out in this Agreement, or in the applicable governing law, rule or policy.

v. Appendices may not be amended to alter the basic purpose or project that an appendix was created for.

C. Agreement Review

i. This Agreement shall be reviewed at least once every State Fiscal Year by representatives from both Parties to ensure that the all provisions of, and references in, this Agreement are up to date and accurately reflect current best practices, rules, and regulations regarding data privacy and security.

D. Appendix Review

i. All appendices shall be reviewed by the party providing the data at least every twelve (12) months to ensure that all information contained in each appendix is complete and accurate. If a program is no longer active the Appendix may be relabeled as inactive or removed, as dictated by the written process agreed to by the Parties.

10. GENERAL PROVISIONS

A. References

All references in this Agreement to sections (whether spelled out or using the § symbol), subsections, exhibits or other attachments, are references to sections, subsections, exhibits or other attachments contained herein or incorporated as a part hereof, unless otherwise noted.

All specific section references to external rules, laws, or polices shall be deemed to reference those sections as they were labeled at the time of the execution of the document.

B. Order of Precedence

i. The provisions of this Agreement shall govern the relationship between the parties. In the event of conflicts or inconsistencies between this Agreement and its

exhibits and attachments, such conflicts or inconsistencies shall be resolved by reference to the documents in the following order of priority:

a. Federal and State Rules, law, regulations and other policies or requirements on how specific data is to be handled.

b. Exhibit D, HIPAA BAA

c. Exhibit F, Combined Limited Dataset and Research DUA

d. The provisions of the main body of this Agreement and Exhibit A, Definitions.

e. Appendices that follow this Agreement

f. Exhibit B, Sample Appendix

g. Exhibit C, Sample Option Letter

h. Exhibit E, Federal Tax Information Requirements Information

C. Compliance with Applicable Law

Parties shall at all times during this Agreement strictly adhere to, and comply with, all applicable Federal and State privacy laws, and their implementing regulations as they currently exist and may hereafter be amended. These laws are incorporated herein by this reference as terms and conditions of this Agreement. Parties shall also require compliance with these statutes and regulations in any subcontracts and sub-grants permitted under this Agreement and its associated Appendices.

D. Third Party Beneficiaries-Negation

Enforcement of all rights and obligations hereunder are reserved solely to the parties. Any services or benefits which third parties receive as a result of this Agreement are incidental and do not create any rights for such third parties.

11. CORA REQUESTS

Parties shall immediately forward any relevant public records requests for shared Data to the Data Provider's principal representative. Departments shall work together to ensure that all requests are handled appropriately.

12. DATA REQUESTS

A. All Data requests shall follow the policy and procedure requirements for requesting Data as described by each Party's Data Governance Plan.

B. Upon approval of the request, prior to any data being shared, Departments shall ensure that a new Appendix is created and added to this Agreement via Amendment. Failure to do so may lead to delays in receipt of the data and possible cancellation of the request.

13. DATA ACCURACY

All data shall be as accurate as possible. Any inaccuracies shall be shared with both Parties, and shall be corrected as soon as possible.

14. DATA GOVERNANCE PLAN

A. Parties shall have in place, and shall create and comply with, a Data Governance Plan.

B. The Data Governance Plan shall be based on industry, federal and state best practices and guidance from the Governor's Data Advisory Board, and other statewide or Federal guidance that may exist.

C. The Data Governance Plan shall be developed and organized in a clear and logical manner, making it easy to locate particular sections of the plan.

D. Any part of the Data Governance Plan that a Party deems to be confidential shall be marked as such.

E. Each Party shall have the right to request a cooperative review of each other's Data Governance plan.

F. If through collaboration, a potential vulnerability is found, the Parties shall work together to ensure that the vulnerability is addressed. Data sharing may be suspended upon the agreement of the Parties while the vulnerability exists.

15. DATA PROVIDER RESPONSIBILITIES

A. The Provider shall maintain ownership and control of the Data, and is responsible for tracking where, when, to whom, and for what purpose Data is transferred through the use of the Appendices attached to this Agreement.

B. The Provider shall securely transmit Protected Data to the Recipient.

16. DATA RECIPIENT RESPONSIBILITIES

A. The Recipient shall not retain any right, title or interest in any of the Data furnished by the Data Provider except as otherwise permitted in this Agreement, the applicable Appendix, or any applicable laws and regulations.

B. Recipient shall use and disclose all Data and implement appropriate privacy and security controls in compliance with this Agreement, their Data Governance Plan, Office of Information Technology (OIT) policies and any and all applicable laws and regulations.

C. Recipient shall ensure that all Authorized Users follow all internal Data policies and any applicable federal and state rules and laws in order to maintain the privacy and security of all Protected Data.

D. If an Authorized User violates any privacy or security requirement, then the Data Recipient shall take corrective action to remediate the situation and ensure future compliance. Continued non-compliant behavior, shall result in Recipient revoking Authorized User's access to the Data.

E. If an Authorized User's ability to access Protected Data is revoked, then the Recipient shall notify the other Party, and the applicable Appendix will be altered as required.

F. The Recipient may only re-disclose with authorization from the Data Governance Manager (or designated authority) of the Data Provider, and then only further disclose

data in an aggregate form that de-identifies or anonymizes the data, or as a Linked Dataset unless specifically permitted by law, and memorialized in the proper Appendix.

G. The Recipient is responsible for ensuring that Data is destroyed or rendered inaccessible upon the completion of its intended use, for which the Data was provided in compliance with applicable rule, law, policy, or the applicable Appendix.

17. DATA PRIVACY & SECURITY

A. All Data privacy and security controls shall comply with the applicable governing authorities including, but not limited to those described in this Agreement and its attachments the Party's Data Governance Plan, and all applicable laws, rules, policies, publications, and guidelines.

B. Any data sharing under this Agreement by consolidated agencies, will comply with the OIT's Information Security Policies issued under the authority of C.R.S. 24-37.5.401-406 and posted on OIT's website.[1]

C. If a more specific or higher protection is required under any applicable rule, law or policy, including those not mentioned, then the Parties shall comply with that rule, law, or policy.

D. All requirements for data management, privacy and security listed herein shall apply to third party vendors performing services for named state agencies, and whom are utilizing the data shared through this Agreement.

E. All data shall be maintained and hosted within the United States.

18. DATA RETENTION

A. All Parties shall only keep shared data as long as they are specifically permitted to under this Agreement and the applicable Appendices.

B. Upon the completion of a program, the Recipient shall destroy or securely sequester all copies of the Protected Data as required by this Agreement or other controlling rules, law or policies.

C. Parties may keep any reports created from the Data unless specifically restricted from doing so.

19. ACCESS RESTRICTIONS

A. The Parties shall ensure that access to the Data covered by this Agreement shall be limited to Authorized Users.

B. The Parties shall ensure that Authorized Users may only have access to the data minimally necessary to complete the work for which the Data was shared.

C. The Parties shall ensure that Data is secured with proper access controls.

D. Recipient may provide Protected Data to its agents, employees, assigns and Subcontractors, whom have been specifically designated as Authorized Users in the

[1] *http://oit.state.co.us/ois/policies*

applicable Appendices, and shall restrict access to Data to those agents, employees, assigns and Subcontractors.

E. Any changes to Authorized Users shall be made in compliance with this Agreement, and shall be recorded in the applicable Appendix.

20. LINKED DATA

A. The Party linking the data shall classify the linked data according to what, if any protected information is contained in the linked data set, and the Risk Assessment procedures described in CISP-013, Risk Assessment.

B. If any protected information will be included in the Dataset to be released, both Parties shall sign off on the release of the Data, and the Agreement providing for the release of the Data.

C. The Party linking and releasing the Data is responsible for ensuring the security of the Data and that all applicable federal and state rules and regulations are followed.

D. The linking Party shall ensure that a release of linked data is accompanied with an Agreement with the 3rd party to ensure the security of the data.

   i. That Agreement shall contain, at minimum:

      a. Insurance requirements obligating the 3rd party to ensure that they are covered in case of breach.

      b. Requirements on the security of transmission, storage and usage which are, at a minimum, compliant with the applicable State and Federal privacy law, as well as the requirements in this Agreement.

      c. A system designed to track what data, and to whom the data is being accessed by, that is substantially similar to the Appendices attached to this Agreement.

E. If any linked Data is to be released to the public, the Party releasing the Data shall be responsible for ensuring that it does not contain any protected information, and shall receive approval from both Parties prior to releasing the Data.

F. Any release of linked Data shall be noted in the appropriate Appendix to this Agreement, and shall describe what Data is shared and to whom.

21. INCIDENTS & REMEDIATION

A. Parties shall make a good faith effort to identify any use or disclosure of confidential Data not authorized by this Agreement.

B. If either Party becomes aware of any Incident involving shared Data, it shall notify the other Party immediately and shall cooperate regarding recovery, mitigation, remediation, and the necessity to involve law enforcement.

C. The Departments shall cooperate in ensuring that the individuals impacted by the Breach or Incident are contacted in accordance with the relevant breach laws and rules.

D. Recipients may not contact such individuals prior to notification of both Parties' management, and a final plan on how the problem will be handled is determined.

E. After an Incident, Parties shall work together to take steps to reduce the risk of a similar type of Incident in the future. These steps may include, but are not limited to, developing and implementing a remediation plan, modification of Data Governance plans and policies, and third-party audit of system and data privacy and security.

22. APPENDICES

A. The structure of the appendices should follow the Sample form attached as Exhibit B, Sample Appendix, to the greatest extent possible.

B. A list of the current and expired Data Sharing Appendices shall be maintained on the State's Contract Management System (CMS).

C. The Data Provider shall be responsible for maintaining those Appendices regarding the Data they are providing in compliance with the processes agreed to by the Parties.

D. Each individual appendix shall describe at least the following:

i. The purpose and scope of the project for which the data is to be shared.

ii. Authority for the disclosure of the Data including any review board approvals.

iii. Program Contacts for both Parties.

iv. A detailed description of the data to be shared which shall include but not be limited to:

a. A description of the dataset or datasets to be shared.

b. A list and brief description of all data elements.

c. The source of the data.

v. Date range for the data is allowed to be shared and retained.

vi. Any applicable Data protection rules or other guidance, as needed.

vii. A list of the specific positions and/or personnel that will have access to the data and be considered Authorized Users.

viii. A list of any outside entities that will have access to any segment of the data.

ix. Any additional protections, constraints definitions, or any other program-specific considerations that are required.

E. The appendices may be added and amended as described in Section 8 of this Agreement.

23. Health Insurance Portability and Accountability Act of 1996 (HIPAA) Business Associate Addendum (BAA)

A. The Colorado Attorney General's approved HIPAA Business Associate Addendum is included as Exhibit D.

B. By signing this Agreement, the Parties agree that they will comply with all terms of the HIPAA BAA when HIPAA protections are applicable to the Data that is being transferred between the Parties.

i. These specific requirements apply when one Party is serving as a Business Associate, as defined in HIPAA.

C. The terms of the HIPAA BAA, when applicable, shall control over any term of this main Agreement.

24. HIPAA LIMITED DATA SET DATA USE AGREEMENT (LDS DUA)

A. The HIPAA LDS DUA shall be applicable only when a limited dataset, as defined under HIPAA, is being provided.

B. By signing this Agreement, the Parties agree that they will comply with all terms of the HIPAA LDS DUA when HIPAA protections are applicable to the Data that is being transferred between the Parties.

C. The terms of the HIPAA LDS DUA, attached as Exhibit F, when applicable, shall control over any term of this main Agreement.

25. HIPAA RESEARCH DATA USE AGREEMENT (DUA), I.E. RESEARCH WRITTEN ASSURANCES

A. The HIPAA Research DUA shall be applicable only when written assurances and a waiver of authorization are required as defined under HIPAA.

B. By signing this Agreement, the Parties agree that they will comply with all terms of the HIPAA Research DUA when HIPAA protections are applicable to the Data that is being transferred between the Parties.

C. The terms of the HIPAA Research DUA, attached as Exhibit F, when applicable, shall control over any term of this main Agreement.

26. FEDERAL TAX INFORMATION (FTI) GUIDANCE

A. Minimal guidance related to the handling of FTI under IRS Publication 1075 is attached to this Agreement as Exhibit E.

B. This guidance does not serve in any way as a definitive description of the requirements or duties required in order to handle FTI, and shall only serve as an informational starting point regarding federal requirements.

C. The Parties are individually and jointly responsible for following federal requirements associated with FTI when applicable.

27. HUMAN SUBJECT RESEARCH

A. Information regarding Human Subject Research shall be governed by 45 CFR 46, 21 CFR 50, and 21 CFR 56 as amended.

B. The Parties shall ensure that all Federal requirements relating to Human Subject Research information are followed.

28. OTHER GUIDANCE AND EXHIBITS

A. From time to time as further guidance and requirements are developed regarding the specific requirements for handling specific types of Protected Information additional exhibits may be included to provide additional requirements and or guidance.

B. Any additional exhibits will be added via amendment.

REMAINDER OF THIS PAGE INTENTIONALLY LEFT BLANK

Exhibit A, Definitions

i. **42 part 2 -** The federal law, contained in 42 CFR part 2, which protects patient records in connection with the performance of any drug and alcohol abuse prevention function.

ii. **Authorized User -** An individual who has been specifically granted the security privileges and rights needed to access a specific set of Data or System.

iii. **Criminal Justice Information (CJI**) - Information collected by criminal justice agencies needed for the performance of their authorized functions, including, without limitation, all information defined as criminal justice information by the U.S. Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services Security Policy, as amended and all Criminal Justice Records as defined under 24-72-302 C.R.S. CJI requires a higher level of security procedures than other Protected Data, as required by OIT.

iv. **Consolidated Agency -** Those state agencies, as defined in C.R.S. 24-37.5-102(4) whose IT functions were consolidated under OIT pursuant to SB 08-155.

v. **CORA** - The Colorado Open Records Act, C.R.S. §§24-72-200.1 *et. seq.*

vi. **Covered Entity –** Under HIPAA, A health plan, health care clearinghouse, or a health care provider who transmits any health information in electronic form in connection with a covered transaction. For the purposes of this agreement HCPF is a Covered Entity.

vii. **Data –** Information stored as text, numbers, graphics, images, sounds, or video. Includes information stored digitally, or by any physical media.

viii. **Data Breach –** An act where an Unauthorized User accesses Protected Data, or when an Authorized User accesses, uses, or releases Protected Data in a way which is not within the scope of their authorized use, or the Protected Data's permissible use.

ix. **Data Recipient (Recipient)** - An individual, organization, or Department, who receives and uses data from the Data Provider.

x. **Data Governance -** The policies and processes which control, at minimum: the assurance of data quality, data security management, business process management, and risk management surrounding the handling of Data.

xi. **Data Governance Manager** - The individual responsible for the implementation and oversight of the Department's Data Governance.

xii. **Data Owner –** The individual, or group, who retain ownership and control of a given Data set. The Data Owner has the responsibility and authority over the operational, technical, and informational management of a Data resource.

xiii. **Data Provider** - The Agency, Department or organization which is providing the Data to be shared.

xiv. **Data Sharing** – The act of transferring data from the Data Provider to the Recipient

xv. **Data Stewards** - The individuals, or organizations, responsible for managing or housing data elements received from the Data Owner or Data Provider in compliance with all rules, regulations, and Agreements.

xvi. **Family Educational Rights and Privacy Act (FERPA)** - The federal law that protects the privacy of education records holding students' personally identifiable information. Contained in 42 USC 1232(g).

xvii. **Dataset** – A collection of Data gathered into a single document or other storage medium.

xviii. **Effective Date** – The date this agreement is signed by the Executive Director of both Departments.

xix. **Health Insurance Portability and Accountability Act of 1996 (HIPAA) –** The federal law that establishes privacy and security standards for Protected Health Information and other patient records. Contained in 45 C.F.R. 160-164

xx. **Incident** - Any accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access or disclosure of Protected Data or of the unauthorized modification, disruption, or destruction of any Protected Data.

xxi. **Linked Data Set -** The resultant Dataset after two or more Departments' data has been combined. Creating a Linked Data Set shall not absolve the parties of their requirements to protect the Data in compliance with this agreement.

xxii. **Non-Consolidated Agencies** - Those state agencies whose IT functions were not consolidated under OIT in SB 08-155.

xxiii. **Payment Card Information** (**PCI**) - Information including any data related to credit card holders' names, credit card numbers, or the other credit card information as may be protected by state or federal law.

xxiv. **Personal Identifying Information (PII)** - Any information about an individual that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and any other information that is linked or linkable

to an individual, such as medical, educational, financial, and employment information. PII includes, but is not limited to, all information defined as personally identifiable information in C.R.S. §24-72-501.

xxv. **Protected Data –** Data that is subject to restrictions on its dissemination and is not subject to disclosure under CORA.

xxvi. **Protected Health Information (PHI) -** Any information, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and (ii) that identifies the individual with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the Privacy Rule, including, but not limited to 45 C.F.R Section 164.501.

xxvii. **Protected Tax Information** - Federal and State of Colorado tax information including, without limitation, federal and State tax returns, return information, and such other tax-related information as may be protected by federal and State law and regulation. Tax Information includes, but is not limited to all information defined as federal tax information in Internal Revenue Service Publication 1075.

xxviii. **Public Health Authority –** An organization that may receive PHI from a Covered Entity without individual authorization that is authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury or disability, such as for purposes of reporting disease, injury, or vital events, or for public health surveillance, investigations, or interventions; or, at the direction of a public health authority, to an official of a foreign government agency that is acting in collaboration with a public health authority.

xxix. **Role-Based Access –** A method of regulating access based on the roles or positions of individual users within an enterprise.

xxx. "**Tax Information**" - Federal and State of Colorado tax information including, without limitation, federal and State tax returns, return information, and such other tax-related information as may be protected by federal and State law and regulation. Tax Information includes, but is not limited to all information defined as federal tax information in Internal Revenue Service Publication 1075.

xxxi. **Unauthorized User** – Any individual who is not an Authorized User.

Exhibit B, Sample Appendix

I. Purpose

A. [Insert a detailed summary of the purpose for requesting the data, to include information about the purpose for requesting the data, what the data will be used for, and any other background applicable to program.]

II. Authority

A. This Data is permitted to be shared [Insert a detailed and specific reason why the data is allowed to be shared including statutory references and IRB approvals as needed]

III. Contacts

A. The program contact for Recipient is [Insert Name, email and phone number].

B. The program contact for Provider is [Insert Name, email and phone number].

C. The Data Governance Manager for Provider is [Insert Name, email and phone number] and the Data Governance Manager for Recipient is [Insert Name, email and phone number].

IV. Data Description

A. The Data covered by this Appendix consists of: [Insert a description of the data to include the dataset, specific data elements, and timeframe which the Data will cover]

B. The Data comes from [Insert a summary of the source of the Data]

C. The Data will be retained for [Insert the dates the Data will be retained]

V. Applicable Regulations

A. The following protection regulations are applicable to the data being transferred:

1. [Insert regulations as applicable]

VI. Authorized Users

A. [Insert the names or position titles of the individuals who can access the raw data]

VII. Third Party Access

A. [Insert the names of the outside entities who will be provided the Data by the Recipient]

Additional:

Constraints,

Definitions,

Confidentiality Requirements,

Program Specific Items,

EXHIBIT C, SAMPLE OPTION LETTER

OPTION LETTER

State Agency Executing the Option	**Option Letter Number** Insert the Option Number (e.g. "1" for the first option)
Other State Agency Insert State Agency Name	**Original Contract Number** Insert CMS number or Other Contract Number of the Original Contract
	Option Contract Number Insert CMS number or Other Contract Number of this Option
	Contract Performance Beginning Date The later of the Effective Date or Month Day, Year

1. OPTION TO AMEND DATA SHARING APPENDIX:

A. In accordance with the provisions of Section 8 of this agreement, the listed Party hereby executes this Option Letter amending the following appendices:
   i. List appendices here

B. The updated appendices are attached to this Option Letter

C. The Party executing this Option shall be responsible for ensuring that this Option and all attachments are provided to the other Party, and all changes are operationalized within the scope of the Agreement.

2. OPTION EFFECTIVE DATE:

A. The effective date of this Option Letter is upon approval of the State Controller or , whichever is later.

STATE OF COLORADO John W. Hickenlooper, Governor Department Executive Director _____ By: Executive Director Date: _____	**STATE CONTROLLER** **Robert Jaros, CPA, MBA, JD** By:_____ Controller; Option Effective Date:_____

Exhibit D, HIPAA BUSINESS ASSOCIATE ADDENDUM

This Business Associate Addendum ("Addendum") is part of the Contract between the Colorado Department of Health Care Policy and Financing (HCPF) and the Colorado Department of Public Health and Environment (CDPHE). For purposes of this Addendum, HCPF is referred to as "Covered Entity" or "CE" and CDPHE is referred to as "Associate". Unless the context clearly requires a distinction between the Contract document and this Addendum, all references herein to "the Contract" or "this Contract" include this Addendum.

RECITALS

A. CE wishes to disclose certain information to Associate pursuant to the terms of the Contract, some of which may constitute Protected Health Information ("PHI") (defined below).

B. CE and Associate intend to protect the privacy and provide for the security of PHI disclosed to Associate pursuant to this Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. §1320d – 1320d-8 ("HIPAA") as amended by the American Recovery and Reinvestment Act of 2009 ("ARRA")/HITECH Act (P.L. 111-005), and its implementing regulations promulgated by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160, 162 and 164 (the "HIPAA Rules") and other applicable laws, as amended.

C. As part of the HIPAA Rules, the CE is required to enter into a contract containing specific requirements with Associate prior to the disclosure of PHI, as set forth in, but not limited to, Title 45, Sections 160.103, 164.502(e) and 164.504(e) of the Code of Federal Regulations ("C.F.R.") and contained in this Addendum.

The parties agree as follows:

1. Definitions.

a. Except as otherwise defined herein, capitalized terms in this Addendum shall have the definitions set forth in the HIPAA Rules at 45 C.F.R. Parts 160, 162 and 164, as amended. In the event of any conflict between the mandatory provisions of the HIPAA Rules and the provisions of this Contract, the HIPAA Rules shall control. Where the provisions of this Contract differ from those mandated by the HIPAA Rules, but are nonetheless permitted by the HIPAA Rules, the provisions of this Contract shall control.

b. "Protected Health Information" or "PHI" means any information, whether oral or recorded in any form or medium: (i) that relates to the past, present or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.501.

c. "Protected Information" shall mean PHI provided by CE to Associate or created, received, maintained or transmitted by Associate on CE's behalf. To the extent Associate is a covered entity under HIPAA and creates or obtains its own PHI for treatment, payment and health care operations, Protected Information under this Contract does not include any PHI created or obtained by Associate as a covered entity and Associate shall follow its own policies and procedures for accounting, access and amendment of Associate's PHI.

d. "Subcontractor" shall mean a third party to whom Associate delegates a function, activity, or service that involves CE's Protected Information, in order to carry out the responsibilities of this Agreement.

2. Obligations of Associate.

a. Permitted Uses. Associate shall not use Protected Information except for the purpose of performing Associate's obligations under this Contract and as permitted under this Addendum. Further, Associate shall not use Protected Information in any manner that would constitute a violation of the HIPAA Rules if so used by CE, except that Associate may use Protected Information: (i) for the proper management and administration of Associate; (ii) to carry out the legal responsibilities of Associate; or (iii) for Data Aggregation purposes for the Health Care Operations of CE. Additional provisions, if any, governing permitted uses of Protected Information are set forth in Attachment A to this Addendum.

b. Permitted Disclosures. Associate shall not disclose Protected Information in any manner that would constitute a violation of the HIPAA Rules if disclosed by CE, except that Associate may disclose Protected Information: (i) in a manner permitted pursuant to this Contract; (ii) for the proper management and administration of Associate; (iii) as required by law; (iv) for Data Aggregation purposes for the Health Care Operations of CE; or (v) to report violations of law to appropriate federal or state authorities, consistent with 45 C.F.R. Section 164.502(j)(1). To the extent that Associate discloses Protected Information to a third party Subcontractor, Associate must obtain, prior to making any such disclosure: (i) reasonable assurances through execution of a written agreement with such third party that such Protected Information will be held confidential as provided pursuant to this Addendum and only disclosed as required by law or for the purposes for which it was disclosed to such third party; and that such third party will notify Associate within five (5) business days of any breaches of confidentiality of the Protected Information, to the extent it has obtained knowledge of such breach. Additional provisions, if any, governing permitted disclosures of Protected Information are set forth in Attachment A.

c. Appropriate Safeguards. Associate shall implement appropriate safeguards as are necessary to prevent the use or disclosure of Protected Information other than as permitted by this Contract. Associate shall comply with the requirements of the HIPAA Security Rule, at 45 C.F.R. Sections 164.308, 164.310, 164.312, and 164.316. Associate shall maintain a comprehensive written information privacy and security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the Associate's operations and the nature and scope of its activities. Associate shall review, modify, and update

documentation of its safeguards as needed to ensure continued provision of reasonable and appropriate protection of Protected Information.

d. Reporting of Improper Use or Disclosure. Associate shall report to CE in writing any use or disclosure of Protected Information other than as provided for by this Contract within five (5) business days of becoming aware of such use or disclosure.

e. Associate's Agents. If Associate uses one or more Subcontractors or agents to provide services under the Contract, and such Subcontractors or agents receive or have access to Protected Information, each Subcontractor or agent shall sign an agreement with Associate containing substantially the same provisions as this Addendum and further identifying CE as a third party beneficiary with rights of enforcement and indemnification from such Subcontractors or agents in the event of any violation of such Subcontractor or agent agreement. The agreement between the Associate and Subcontractor or agent shall ensure that the Subcontractor or agent agrees to at least the same restrictions and conditions that apply to Associate with respect to such Protected Information. Associate shall implement and maintain sanctions against agents and Subcontractors that violate such restrictions and conditions and shall mitigate the effects of any such violation.

f. Access to Protected Information. If Associate maintains Protected Information contained within CE's Designated Record Set, Associate shall make Protected Information maintained by Associate or its agents or Subcontractors in such Designated Record Sets available to CE for inspection and copying within ten (10) business days of a request by CE to enable CE to fulfill its obligations to permit individual access to PHI under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.524. If such Protected Information is maintained by Associate in an electronic form or format, Associate must make such Protected Information available to CE in a mutually agreed upon electronic form or format.

g. Amendment of PHI. If Associate maintains Protected Information contained within CE's Designated Record Set, Associate or its agents or Subcontractors shall make such Protected Information available to CE for amendment within ten (10) business days of receipt of a request from CE for an amendment of Protected Information or a record about an individual contained in a Designated Record Set, and shall incorporate any such amendment to enable CE to fulfill its obligations with respect to requests by individuals to amend their PHI under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.526. If any individual requests an amendment of Protected Information directly from Associate or its agents or Subcontractors, Associate must notify CE in writing within five (5) business days of receipt of the request. Any denial of amendment of Protected Information maintained by Associate or its agents or Subcontractors shall be the responsibility of CE.

h. Accounting Rights. Associate and its agents or Subcontractors shall make available to CE, within ten (10) business days of notice by CE, the information required to provide an accounting of disclosures to enable CE to fulfill its obligations under the HIPAA Rules, including, but not limited to, 45 C.F.R. Section 164.528. In the event that the request for an accounting is delivered directly to Associate or its agents or Subcontractors, Associate shall within five (5) business days of the receipt of the request, forward it to CE in writing. It shall be

CE's responsibility to prepare and deliver any such accounting requested. Associate shall not disclose any Protected Information except as set forth in Section 2(b) of this Addendum.

i. Governmental Access to Records. Associate shall keep records and make its internal practices, books and records relating to the use and disclosure of Protected Information available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary"), in a time and manner designated by the Secretary, for purposes of determining CE's or Associate's compliance with the HIPAA Rules. Associate shall provide to CE a copy of any Protected Information that Associate provides to the Secretary concurrently with providing such Protected Information to the Secretary when the Secretary is investigating CE. Associate shall cooperate with the Secretary if the Secretary undertakes an investigation or compliance review of Associate's policies, procedures or practices to determine whether Associate is complying with the HIPAA Rules, and permit access by the Secretary during normal business hours to its facilities, books, records, accounts, and other sources of information, including Protected Information, that are pertinent to ascertaining compliance.

j. Minimum Necessary. Associate (and its agents or Subcontractors) shall only request, use and disclose the minimum amount of Protected Information necessary to accomplish the purpose of the request, use or disclosure, in accordance with the Minimum Necessary requirements of the HIPAA Rules including, but not limited to, 45 C.F.R. Sections 164.502(b) and 164.514(d).

k. Data Ownership. Associate acknowledges that Associate has no ownership rights with respect to the Protected Information.

l. Retention of Protected Information. Except upon termination of the Contract as provided in Section 4(c) of this Addendum, Associate and its Subcontractors or agents shall retain all Protected Information throughout the term of this Contract and shall continue to maintain the information required under Section 2(h) of this Addendum for a period of six (6) years.

m. Associate's Insurance. Associate shall maintain insurance to cover loss of PHI data and claims based upon alleged violations of privacy rights through improper use or disclosure of PHI. All such policies shall meet or exceed the minimum insurance requirements of the Contract (e.g., occurrence basis, combined single dollar limits, annual aggregate dollar limits, additional insured status and notice of cancellation).

n. Notification of Breach. During the term of this Contract, Associate shall notify CE within five (5) business days of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of Protected Information and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. Associate shall not initiate notification to affected individuals per the HIPAA Rules without prior notification and approval of CE. Information provided to CE shall include the identification of each individual whose unsecured PHI has been, or is reasonably believed to have been accessed, acquired or disclosed during the breach. Associate shall take (i) prompt corrective action to cure

any such deficiencies and (ii) any action pertaining to such unauthorized disclosure required by applicable federal and state laws and regulations.

o. Audits, Inspection and Enforcement. Within ten (10) business days of a written request by CE, Associate and its agents or Subcontractors shall allow CE to conduct a reasonable inspection of the facilities, systems, books, records, agreements, policies and procedures relating to the use or disclosure of Protected Information pursuant to this Addendum for the purpose of determining whether Associate has complied with this Addendum; provided, however, that: (i) Associate and CE shall mutually agree in advance upon the scope, timing and location of such an inspection; and (ii) CE shall protect the confidentiality of all confidential and proprietary information of Associate to which CE has access during the course of such inspection. The fact that CE inspects, or fails to inspect, or has the right to inspect, Associate's facilities, systems, books, records, agreements, policies and procedures does not relieve Associate of its responsibility to comply with this Addendum, nor does CE's (i) failure to detect or (ii) detection, but failure to notify Associate or require Associate's remediation of any unsatisfactory practices, constitute acceptance of such practice or a waiver of CE's enforcement rights under the Contract.

p. Safeguards During Transmission. Associate shall be responsible for using appropriate safeguards, including encryption of PHI, to maintain and ensure the confidentiality, integrity and security of Protected Information transmitted to CE pursuant to the Contract, in accordance with the standards and requirements of the HIPAA Rules.

q. Restrictions and Confidential Communications. Within ten (10) business days of notice by CE of a restriction upon uses or disclosures or request for confidential communications pursuant to 45 C.F.R. Section 164.522, Associate will restrict the use or disclosure of an individual's Protected Information. Associate will not respond directly to an individual's requests to restrict the use or disclosure of Protected Information or to send all communication of Protected Information to an alternate address. Associate will refer such requests to the CE so that the CE can coordinate and prepare a timely response to the requesting individual and provide direction to Associate.

3. Obligations of CE.

a. Safeguards During Transmission. CE shall be responsible for using appropriate safeguards, including encryption of PHI, to maintain and ensure the confidentiality, integrity and security of Protected Information transmitted pursuant to this Contract, in accordance with the standards and requirements of the HIPAA Rules.

b. Notice of Changes. CE maintains a copy of its Notice of Privacy Practices on its website. CE shall provide Associate with any changes in, or revocation of, permission to use or disclose Protected Information, to the extent that it may affect Associate's permitted or required uses or disclosures. To the extent that it may affect Associate's permitted use or disclosure of PHI, CE shall notify Associate of any restriction on the use or disclosure of Protected Information that CE has agreed to in accordance with 45 C.F.R. Section 164.522.

4. Termination.

a. Material Breach. In addition to any other provisions in the Contract regarding breach, a breach by Associate of any provision of this Addendum, as determined by CE, shall constitute a material breach of this Contract and shall provide grounds for immediate termination of this Contract by CE pursuant to the provisions of the Contract covering termination for cause, if any. If the Contract contains no express provisions regarding termination for cause, the following terms and conditions shall apply:

(1) Default. If Associate refuses or fails to timely perform any of the provisions of this Contract, CE may notify Associate in writing of the non-performance, and if not promptly corrected within the time specified, CE may terminate this Contract. Associate shall continue performance of this Contract to the extent it is not terminated and shall be liable for excess costs incurred in procuring similar goods or services elsewhere.

(2) Associate's Duties. Notwithstanding termination of this Contract, and subject to any directions from CE, Associate shall take timely, reasonable and necessary action to protect and preserve property in the possession of Associate in which CE has an interest.

b. Reasonable Steps to Cure Breach. If CE knows of a pattern of activity or practice of Associate that constitutes a material breach or violation of the Associate's obligations under the provisions of this Addendum or another arrangement, then CE shall take reasonable steps to cure such breach or end such violation. If CE's efforts to cure such breach or end such violation are unsuccessful, CE shall terminate the Contract, if feasible. If Associate knows of a pattern of activity or practice of a Subcontractor or agent that constitutes a material breach or violation of the Subcontractor's or agent's obligations under the written agreement between Associate and the Subcontractor or agent, Associate shall take reasonable steps to cure such breach or end such violation, if feasible.

c. Effect of Termination.

(1) Except as provided in paragraph (2) of this subsection, upon termination of this Contract, for any reason, Associate shall return or destroy all Protected Information that Associate or its agents or Subcontractors still maintain in any form, and shall retain no copies of such Protected Information. If Associate elects to destroy the Protected Information, Associate shall certify in writing to CE that such Protected Information has been destroyed.

(2) If Associate believes that returning or destroying the Protected Information is not feasible, Associate shall promptly provide CE notice of the conditions making return or destruction infeasible. Associate shall continue to extend the protections of Sections 2(a), 2(b), 2(c), 2(d) and 2(e) of this Addendum to such Protected Information, and shall limit further use of such PHI to those purposes that make the return or destruction of such PHI infeasible.

5. Injunctive Relief. CE shall have the right to injunctive and other equitable and legal relief against Associate or any of its Subcontractors or agents in the event of any use or disclosure of Protected Information in violation of this Contract or applicable law.

6. No Waiver of Immunity. No term or condition of this Contract shall be construed or interpreted as a waiver, express or implied, of any of the immunities, rights, benefits, protection, or other provisions of the Colorado Governmental Immunity Act, CRS 24-10-101 *et seq*. or the Federal Tort Claims Act, 28 U.S.C. 2671 *et seq*. as applicable, as now in effect or hereafter amended.

7. Limitation of Liability. Any limitation of Associate's liability in the Contract shall be inapplicable to the terms and conditions of this Addendum.

8. Disclaimer. CE makes no warranty or representation that compliance by Associate with this Contract or the HIPAA Rules will be adequate or satisfactory for Associate's own purposes. Associate is solely responsible for all decisions made by Associate regarding the safeguarding of PHI.

9. Certification. To the extent that CE determines an examination is necessary in order to comply with CE's legal obligations pursuant to the HIPAA Rules relating to certification of its security practices, CE or its authorized agents or contractors, may, at CE's expense, examine Associate's facilities, systems, procedures and records as may be necessary for such agents or contractors to certify to CE the extent to which Associate's security safeguards comply with the HIPAA Rules or this Addendum.

10. Amendment.

a. Amendment to Comply with Law. The parties acknowledge that state and federal laws relating to data security and privacy are rapidly evolving and that amendment of this Addendum may be required to provide for procedures to ensure compliance with such developments. The parties specifically agree to take such action as is necessary to implement the standards and requirements of the HIPAA Rules and other applicable laws relating to the confidentiality, integrity, availability and security of PHI. The parties understand and agree that CE must receive satisfactory written assurance from Associate that Associate will adequately safeguard all Protected Information and that it is Associate's responsibility to receive satisfactory written assurances from Associate's Subcontractors and agents. Upon the request of either party, the other party agrees to promptly enter into negotiations concerning the terms of an amendment to this Addendum embodying written assurances consistent with the standards and requirements of the HIPAA Rules or other applicable laws. CE may terminate this Contract upon thirty (30) days written notice in the event (i) Associate does not promptly enter into negotiations to amend this Contract when requested by CE pursuant to this Section, or (ii) Associate does not enter into an amendment to this Contract providing assurances regarding the safeguarding of PHI that CE, in its sole discretion, deems sufficient to satisfy the standards and requirements of the HIPAA Rules.

b. Amendment of Attachment A. Attachment A may be modified or amended by mutual agreement of the parties in writing from time to time without formal amendment of this Addendum.

11. Assistance in Litigation or Administrative Proceedings. Associate shall make itself, and any Subcontractors, employees or agents assisting Associate in the performance of its obligations under the Contract, available to CE, at no cost to CE, up to a maximum of thirty (30) hours, to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings being commenced against CE, its directors, officers or employees based upon a claimed violation of the HIPAA Rules or other laws relating to security and privacy or PHI, in which the actions of Associate are at issue, except where Associate or its Subcontractor, employee or agent is a named adverse party.

12. No Third Party Beneficiaries. Nothing express or implied in this Contract is intended to confer, nor shall anything herein confer, upon any person other than CE, Associate and their respective successors or assigns, any rights, remedies, obligations or liabilities whatsoever.

13. Interpretation and Order of Precedence. The provisions of this Addendum shall prevail over any provisions in the Contract that may conflict or appear inconsistent with any provision in this Addendum. Together, the Contract and this Addendum shall be interpreted as broadly as necessary to implement and comply with the HIPAA Rules. The parties agree that any ambiguity in this Contract shall be resolved in favor of a meaning that complies and is consistent with the HIPAA Rules. This Contract supersedes and replaces any previous separately executed HIPAA addendum between the parties.

14. Survival of Certain Contract Terms. Notwithstanding anything herein to the contrary, Associate's obligations under Section 4(c) ("Effect of Termination") and Section 12 ("No Third Party Beneficiaries") shall survive termination of this Contract and shall be enforceable by CE as provided herein in the event of such failure to perform or comply by the Associate. This Addendum shall remain in effect during the term of the Contract including any extensions.

ATTACHMENT A

This Attachment sets forth additional terms to the HIPAA Business Associate Addendum, which is part of the Contract between the Colorado Department of Health Care Policy and Financing (HCPF) and the Colorado Department of Public Health and Environment (CDPHE) and is effective as of the date of the Contract (the "Attachment Effective Date"). This Attachment may be amended from time to time as provided in Section 10(b) of the Addendum.

1. Additional Permitted Uses. In addition to those purposes set forth in Section 2(a) of the Addendum, Associate may use Protected Information as follows:

No additional permitted uses.

2. Additional Permitted Disclosures. In addition to those purposes set forth in Section 2(b) of the Addendum, Associate may disclose Protected Information as follows:

No additional permitted disclosures.

3. Subcontractor(s). The parties acknowledge that the following subcontractors or agents of Associate shall receive Protected Information in the course of assisting Associate in the performance of its obligations under this Contract:

No subcontractors.

4. Receipt. Associate's receipt of Protected Information pursuant to this Contract shall be deemed to occur as follows and Associate's obligations under the Addendum shall commence with respect to such Protected Information upon such receipt:

Upon receipt of PHI.

5. Additional Restrictions on Use of Data. CE is a Business Associate of certain other Covered Entities and, pursuant to such obligations of CE, Associate shall comply with the following restrictions on the use and disclosure of Protected Information:

No additional restrictions on Use of Data.

6. Additional Terms. This may include specifications for disclosure format, method of transmission, use of an intermediary, use of digital signatures or PKI, authentication, additional security or privacy specifications, de-identification/re-identification of data, etc.

No additional terms.

Exhibit E, Federal Tax Information Requirements Information

Key Elements of IRS Publication 1075 for Contracts & Procurement

Definition

Federal Tax Information (FTI) includes return and return information received directly from the IRS or obtained through an authorized secondary source, such as the Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS). FTI includes any information created by the recipient that is derived from federal return or return information received from the IRS or obtained through a secondary source.

Background Investigation Minimum Requirements

State and local agencies which are not required to implement the federal background investigation standards must establish a personnel security program, prior to permitting access to FTI, that ensures a background investigation is completed at the appropriate level for all employees and contractors who will have access to FTI, using the guidance below as the minimum standard, and a reinvestigation conducted within 10 years at a minimum.

Agencies must develop a written policy requiring that employees, contractors and sub-contractors (if authorized), with access to FTI must complete a background investigation that is favorably adjudicated. The policy will identify the process, steps, timeframes and favorability standards that the agency has adopted. The agency may adopt the favorability standards set by the FIS or one that is currently used by another state agency, or the Agency may develop its own standards specific to FTI access.

The written background investigation policy must establish a result criterion for each required element which defines what would result in preventing or removing an employee's or contractor's access to FTI.

Agencies must make written background investigation policies and procedures as well as a sample of completed employee and contractor background investigations available for inspection upon request.

Background investigations for any individual granted access to FTI must include, at a minimum:

a) FBI fingerprinting (FD-258) - review of Federal Bureau of Investigation (FBI) fingerprint results conducted to identify possible suitability issues. (Contact the appropriate state identification bureau for the correct procedures to follow.) A listing of state identification bureaus can be found at: https://www.fbi.gov/about-us/cjis/identity-history-summary- checks/state-identification-bureau-listing
This national agency check is the key to evaluating the history of a prospective candidate for access to FTI. It allows the Agency to check the applicant's criminal history in all 50 states, not only current or known past residences.

b) Check of local law enforcement agencies where the subject has lived, worked, and/or attended school within the last 5 years, and if applicable, of the appropriate agency for any identified arrests.

The local law enforcement check will assist agencies in identifying trends of misbehavior that may not rise to the criteria for reporting to the FBI database but is a good source of information regarding an applicant.

c) Citizenship/residency – Validate the subject's eligibility to legally work in the United States (e.g., a United States citizen or foreign citizen with the necessary authorization).

Employers must complete USCIS Form I-9 to document verification of the identity and employment authorization of each new employee hired after November 16, 1986, to work in the United States. Within 3 days of completion, any new employee must also be processed through E-Verify to assist with verification of his/her status and the documents provided with the Form I-9. The E-Verify system is free of charge and can be located at www.uscis.gov/e-verify. This verification process may only be completed on new employees. Any employee with expiring employment eligibility must be documented and monitored for continued compliance.

45-Day Notification Reporting Requirements

All agencies intending to re-disclose FTI to contractors must notify the IRS at least 45 days prior to the planned re-disclosure. Contractors consist of but are not limited to cloud computing providers, consolidated data centers, off-site storage facilities, shred companies, IT support, or tax modeling/revenue forecasting providers. The contractor notification requirement also applies in the circumstance where the contractor hires additional subcontractor services.

Approval is required if the (prime) contractor hires additional subcontractor services in accordance with Exhibit 6, Contractor 45-Day Notification Procedures.

Exhibit 7: Safeguarding Contract Language

Include contract language for general services or contract language for technology services as appropriate. Language changed to add additional requirements in Section I Performance and Section III Inspection.

Implementing IRS Publication 1075

- Development of legislation
    - Due to federal executive order, the FBI may only release information from its database if a state statute authorizes the release. At present, no Colorado state statute authorizes this release for Publication 1075 purposes.
- Development of a model policy and, subsequently, agency specific policies

    - C.R.S. 24-5-101 lays out four criteria that state agencies must consider before disqualifying an individual from employment for a criminal conviction. Most important criteria are the question of how a conviction would impact an individual's ability to perform their job function. Agencies will have to balance, when they encounter a conviction, that factor along with the other three.
- Development of a process to fingerprint employees and contractors
    - Paper ink cards or electronic fingerprints sent to Colorado Bureau of Investigation
- Seek clarification on local law enforcement checks
    - IRS state that a state background check conducted by a third-party vendor would be sufficient to meet this requirement.
    - IRS conveyed that all you have to do is try to get the information from a local law enforcement agency by sending a form. Alternatively, a check of state criminal history will likely suffice.
    - RFP for State Price Agreement for Background Screening Services closes 1/25/17
- Seek clarification on how to handle contractors/subcontractors in other states and/or countries
    - For FBI fingerprinting requirement, due to barriers keeping states from sharing criminal justice information, states will have to individually check contractors with access to FTI. Given the patchwork of Livescan machines and varying willingness to let outside agencies use those machines, out of state contractors will likely have to have their prints rolled manually, have the cards mailed to CBI, and then have the results released to the agency requesting the check.
- Seek clarification on requirement to reinvestigate every 10 years at a minimum
    - The Rap Back system could potentially eliminate the need to do the fingerprint-based background checks every ten years, according to the IRS. What's less clear is whether the local law enforcement check and the citizenship/residency investigation needs also to be performed every ten years, as well.
- Seek clarification on how to handle the requirement to validate existing contractors' and subcontractors' eligibility to work in the U.S.
    - How is this accomplished?
- Interim approach used by DOL
    - Contract language for background checks
    - Background Check Affidavit Form

Exhibit F Combined Limited Dataset and Research DUA

Data Use Agreement

Mandatory for Limited Data Set Requests and Research Requests where a waiver of HIPAA authorization has been reviewed and approved by an Institutional Review Board (IRB).

This Agreement sets forth the terms and conditions pursuant to which Covered Entity will disclose certain protected health information (PHI) to the Data Recipient for purposes of the request described herein.

Covered Entity Obligations:

Covered Entity will agree to provide information to the Data User.

Data User's Obligations:

a. *Uses and disclosures as provided in this Agreement*. Data User may use and disclose the confidential information provided by Covered Entity only for the activity described above. Only the individuals or classes of individuals will have access to the data that need access to the confidential information to do the work as presented in the Agreement.

b. *Nondisclosure Except as Provided in this Agreement.* Data User shall not use or further disclose the confidential data except as per this Agreement and in response to a subpoena or subpoena *duces tecum*, once court-ordered to disclose the information pursuant to 45 C.F.R. 164.512(a); and to fulfill obligations under C.R.S §42-4-1301.3(3) and (4),.

c. *Follow-Back.* Data User may not contact the subject of the information, next-of-kin, the physician, other provider, or any other relative or interested party except as follows: as necessary in monitoring client's compliance with court orders.

d. *Safeguards.* Data User agrees to take appropriate administrative, technical and physical safeguards to protect the data from any unauthorized use or disclosure not provided for in this agreement.

    1) Ensure that no identifying information will be transmitted through unsecured telecommunications, including the unsecured Internet connections.
    2) Ensuring that PHI is encrypted using a FIPS 140-2 compliant algorithm if it is transported across a public network such as the Internet.
    3) Ensuring that PHI is encrypted if it is stored on or accessed from any portable media or device, including, but not limited to, laptops, CD's/DVD's, USB drives, tablets or smartphones/PDA's.

4) Restricting access to any PHI stored on a network such that only individuals directly associated with project and who are aware of this Agreement have access to the data.
5) Maintaining appropriate anti-virus protection on all systems handling or accessing data.
6) Maintain all record retention policies and immediately destroy all copies of data at the conclusion of the project, per any applicable regulatory requirements.

e. *Confidentiality Agreements.* Data User will ensure that all persons who have access to the confidential information sign a confidentiality agreement, and send it to Covered Entity to be assigned a unique user identification number and password. This includes, but is not limited to all interns, sub-contractors, staff, other workforce members, and consultants. Copies of the signed confidentiality agreements shall be maintained on file and be available for review by Covered Entity if requested.

f. *Reporting.* Data User shall report to Covered Entity within 48 hours of Data User becoming aware of any use or disclosure of the confidential information in violation of this Agreement or applicable law.

g. *Public Release.* No confidential information will be publicly released.

h. *Minimum Necessary.* Data User attests that the confidential information requested represents the minimum necessary information for the work and that only the minimum necessary individuals will have access to the confidential information in order to perform the work.

1. *Institutional Review Board (IRB).* An Institutional Review Board is an administrative body established to protect the rights and welfare of human research subjects, including the protection of the subjects' privacy, for research conducted under the auspices of the Data Recipient. The Data Recipient agrees to furnish all documentation concerning IRB reviews, and to submit required documentation to an IRB or Privacy Board should research protocols change. Data Recipient's agrees to submit to the Covered Entity any change in waiver status or conditions for approval of the project by an IRB relating to the work described in the Application. The Covered Entity accepts the IRB's determination, acting in its capacity as a privacy board, to issue a waiver of individual authorization for release of PHI pursuant to HIPAA regulations pertaining to the use of PHI in research (45 CFR section 164.512 (i)).

i. *Authorizations.* Data Recipient agrees to secure individual authorizations to the confidential information for all research projects unless an IRB has approved a waiver of an authorization. Documentation must be provided prior to receipt of the confidential information.

j. *Data Ownership.* Covered Entity is the data owner. The Data User does not obtain any right, title, or interest in any of the data furnished by Covered Entity.

k. *Publication/release requirements.* No PHI (Protected Health Information) Data will be published.

l. *Subcontractors.* Data Recipient agrees to ensure that any partner or agent, including a subcontractor, to whom it provides the PHI, agrees to the same restrictions and conditions that apply through this Agreement to the Data Recipient with respect to such information.

m. *Additional terms.*