Colorado Information Marketplace

Enabling Technology Solutions Efficiently, Effectively, and Elegantly

12/12/2011

Executive Summary

"Errors using inadequate data are much less than those using no data at all."
Charles Babbage

In the last few years, government at all levels has been increasing information availability and collaboration among the various entities in an effort to usher in a new era of effectiveness, efficiency and transparency. Through the Open Government Directive of 2009, the federal government required government agencies to take immediate steps to achieve key milestones in transparency, participation and collaboration. Over the last two years, Colorado has taken steps to stay on the forefront of this initiative by passing various laws and initiatives, such as the Transparency Openness Project System, to ensure a transparent and collaborative government.

We also understand the critical nature of timely, accurate information. Even something as simple as an inaccurate gas indicator in your car could cause you significant annoyance and disruption, especially if you were to run out of gas during rush hour. Every day, we rely on information - from knowing the time of day, to ensuring our new doctor is aware of all of our medical history. And while accurate information is a critical component to our livelihood, combining this information in new ways and with new data points can create an entirely new perspective and change the way we make decisions.

Sharing information across boundaries will improve decision-making, mission performance, and customer service. Additionally, centralizing governance, security and standards around the information will reduce misinterpretation of data and provide the structure for ongoing, secure and reusable information exchanges. The Colorado Information Marketplace will create the architectural framework for those information exchanges by making data visible, accessible, understandable and, above all, trusted.

Table of Contents

Colorado Information Marketplace

Enabling Technology Solutions Efficiently, Effectively, and Elegantly

Current Information Exchange in the State of Colorado

The current environment for data sharing in the state remains disparate and misaligned. Currently, data sharing initiatives are created for one time projects and there are few all encompassing agreements between agencies as it pertains to data sharing. Government agencies waste time, energy, and money locating and cataloging data each time a new data exchange is warranted, either through legislation, grants, or in order to provide intelligence for proper decision making. Lessons learned from past data sharing efforts are rarely available and that lack of knowledge management drives the costs associated with each initiative, as well as the opportunity to misinterpret the data.

Furthermore, several external entities, such as universities, healthcare providers and other public service based organizations, lack access to necessary data that could help them improve services to citizens.

Colorado has passed some legislation in the past few years to improve data sharing. The Government Data Advisory Board (GDAB) was created through HB 09-1285 with the purpose of advising the State's Chief Information Officer on activities and policies necessary to developing the interdepartmental data protocols created in HB 08-1364 and ease the taxing processes of data sharing and exchange. Most government agencies and some external entities are represented on the GDAB, which meets monthly.

Further information on the GDAB may be found here:

http://www.colorado.gov/cs/Satellite/OIT-EADG/CBON/1251579896288

The GDAB has been successful in creating protocols and documentation around data sharing, but the state has yet to embrace the concept of reusable information exchanges. The Colorado Information Marketplace provides a framework for these exchanges with the intent to move us forward in this direction. The office of the State's Chief Technology Officer will use the GDAB as a mining and feedback mechanism for gathering new requirements, information and support within the agency community.

Colorado Information Marketplace Goals

The Colorado Information Marketplace (CIM) has four simple goals, which align with the overall Enterprise Architecture Roadmap for 2011-2014.

1. Improve information availability and interoperability within the state
    a. A consistent view of information over time
    b. A catalog of information available to state agencies, including the governance and standards around the information
    c. Improved availability of data that cannot be shared in its raw form, but that could be made available in aggregate for analysis and reporting

2. Reduce costs and redundancy
    a. Standards and services for reuse
    b. Reduce capture of data when it already exists and is available
    c. Reduce training of analysts around information interpretation
3. Increase information agility
    a. Information is available for real time reporting
    b. Catalog outlines the interpretation of the data
    c. Ability for users to access specific, custom sets of data through a self-service portal
4. Increase information security
    a. Governance models cover the data and are consistent across databases
    b. Information security policies and practices follow industry, federal and state standards (i.e. HIPPA, FERPA)
    c. Roles Based Access Control (RBAC) around who may access and use the data
    d. Auditable information around access and reporting

A Fundamental Shift around Information

The Colorado Information Marketplaces addresses the need to shift focus from siloed data exchanges, which can be prone to misinterpretation, inaccuracy, and risk. Instead, the Colorado Information Marketplace relies on existing data standards, such as the National Information Exchange Model and a governance model to create a reusable source of information for both state, local, county, city, tribal and other external entities that qualify for access and use of the data. The CIM framework applies both consistency of data standards and governance for privacy and security, while improving data transparency and reuse. Mission critical information empowers people to make better decisions in a real time (or near real time) environment, rather than waiting months or, in some cases, years to get access to the right data. Information exchanges will benefit every agency with the State, which will in turn benefit every citizen.

Improving the public sector through the CIM

Providing access to information previously unavailable will transform government's decision-making process through better use of analytics and reporting. And, providing information in a more agile, user-friendly environment will give policy makers the right information at the right time to improve government services.

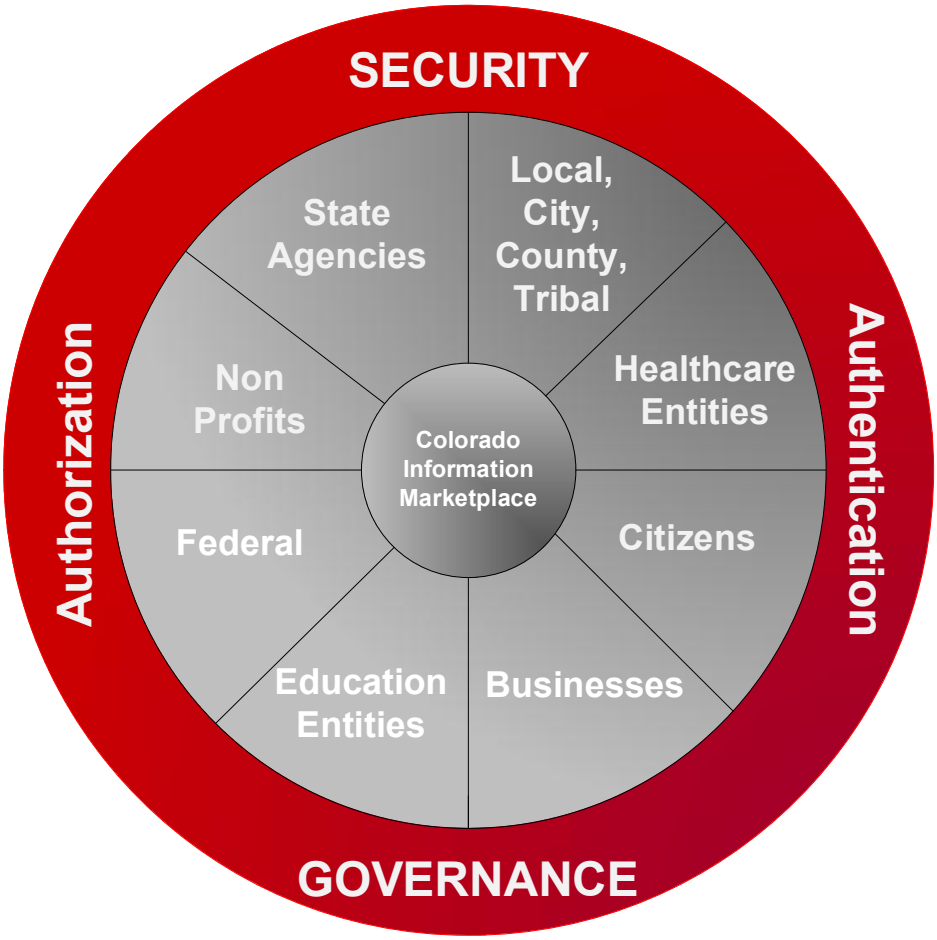
Greater sharing of data will better serve the public with programs that reflect the highest degree of efficiency, coordination, and accountability. Some of the potential benefits of data sharing include:

ÅTimely and improved access to reliable and high-quality data to inform decision-making by the Executive Branch, as well as the Legislature, and other governmental entities.

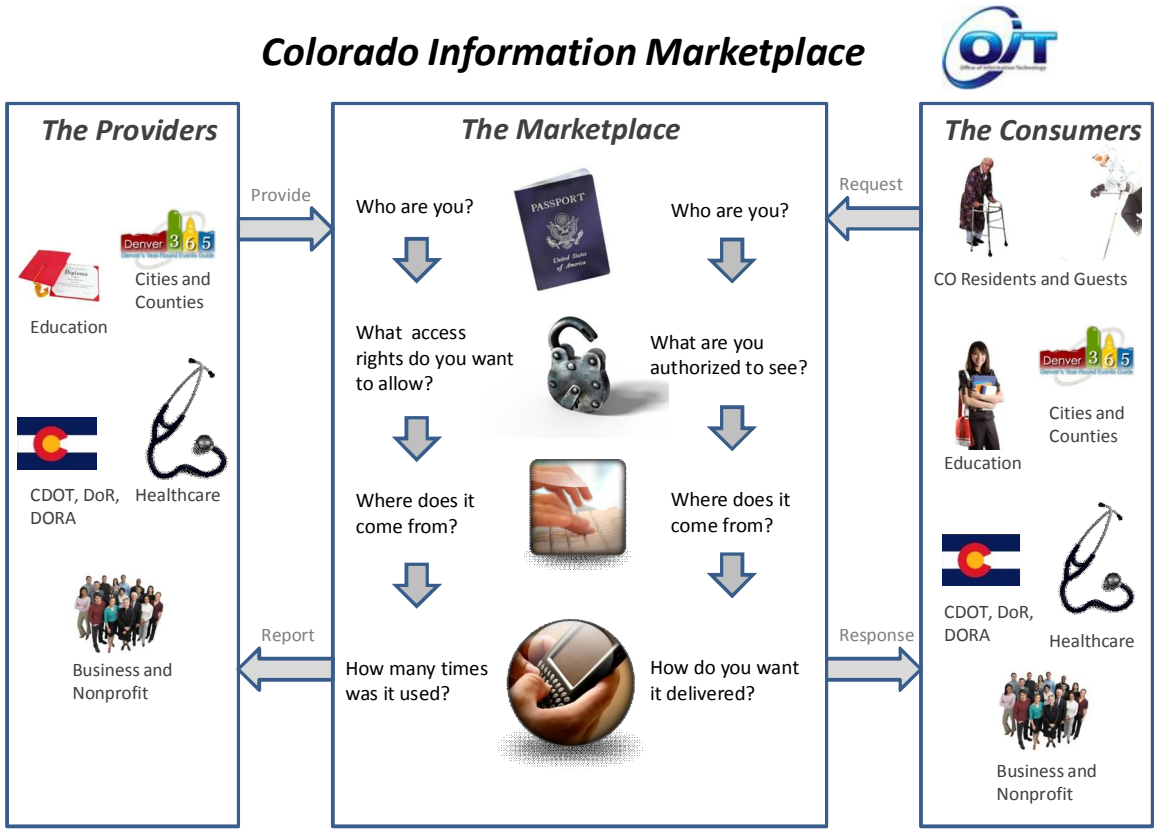
ÅIncreased transparency, better service, and reduced risk of waste, fraud, and abuse with respect to public programs that will increase the publicôs confidence in government.

ÅMore informed research on public policy as a result of an increased number of studies and theorems that rigorously analyze, and augment the understanding of state programs within government for the public at large.

ÅImproved government efficiency as a result of more informed decision-making, collaboration and a reduction in burdensome, excessive, and duplicative data-collection activities.



Decision Framework for the Colorado Information Marketplace



Participation

There are three rules for CIM participation.

1. *Any entity wishing to use the CIM is required to contribute data to the CIM except if the data is made specifically for public entities, then the public entities do not have to contribute back to CIM.*
    a. Since some data is highly regulated and/or sensitive, an entity may only need to contribute aggregate forms of data and information. See data standards and governance sections for more information on this topic.
2. *Participants control the governance of their contributed data in terms of who may access, what they may access and when.*
    a. As regulations and legislation changes, the participants may modify any and all governance around their information.
3. *Participants must provide data sources, definitions data calculations, and other disclosures for correct interpretation and use of the data.*

Selecting Participants

State Agencies

All Colorado state agencies are automatically approved to participate in the CIM, as long as they contribute some data to CIM and conform to state data and information security standards.

Local Entities

Local, city and county entities are included in the CIM, but must show what data they wish to access, as well as how they will meet the security policies set forth for the CIM, including secure access, use of data in motion and at rest, and destruction of data.

Non Government Agencies

Non-government entities and individuals are required to request access from the Office of Information Technology, as well as the specific agencies that own the data, and pass our security policies prior to being allowed access.

The access request form may be accessed in Appendix B

Security Standards

The Colorado Information Marketplace will adhere to all policies and standards set forth by the Chief Information Security Officer for the State of Colorado. Any entity unable to ensure adherence will removed from the CIM.

Policies are found here:

http://www.colorado.gov/oit/security_policies

Standards are found here:

http://www.colorado.gov/oit/security_standards

For information on access and authorization, please refer to the Data Stewards section.

Data Standards

Data standards *are documented agreements on representations, formats, and definitions of common data.*

The Colorado Information Marketplace will place priority on existing standards as they exist via the following organizations:

- National Information Exchange Model (www.niem.gov)
- Federal Government (all agencies and departments that publish a particular standard, including www.data.gov)
- American National Standards Institute (ANSI) (www.ansi.org)
- Existing Reference Architectures

If the State must create one for any information that is not standardized, the state will publish this standard and conform to www.niem.gov requirements, as well as any additional standards that may form the basis for the new standard.

NOTE: Entities will likely have much more data than they are exposing to the CIM. They may have hundreds of data points, but only a few are relevant for use by CIM.

Definitions

It is critical to have a common understanding of what is meant by data governance and stewardship and the potential roles in data stewardship to arrive at standard data stewardship processes. These definitions provide a framework and guidance to agencies in embarking on data stewardship efforts

1. Data Governance

   Data Governance refers to the operating discipline for managing data and information as a key enterprise asset. This operating discipline includes organization, processes and tools for establishing and exercising decision rights regarding valuation and management of data. Key aspects of data governance include decision making authority, compliance monitoring, policies and standards, data inventories, full lifecycle management, content management, records management, preservation, data quality, data classification, data security and access, data risk management, and data valuation.

2. Data Stewardship

   Data stewardship is the practice of managing data and providing users access to that data. Processes supporting enterprise data stewardship will be based on clear, inclusive, and well-documented data architecture. Enterprise data should be shared widely among the primary and secondary user community with proper consideration to sensitivity, legal, and policy concerns that may restrict access and distribution.

4. Data Steward Coordinator

   Selects data, policy, system stewards within their within their organizations who are responsible for the governance and policies around their data. These entities (whether individual, board or other entity type) will address the business policies, procedures, and governance of the information.

5. Data Steward

   An individual or staff that has data knowledge about the program.

6. System Steward

   An individual or staff that has system knowledge about the program.

7. Policy Steward

   An individual or staff that has policy knowledge about the program.

8. Primary Data User

   Primary data users are the agencies, persons, or processes that tie directly to line-of-business functions. Primary users are the primary reason the enterprise data is produced and are the high priority customers for the data. There is often a formal agreement, contract, or mandate between the agency or group providing the data and the data users. For example, the Federal Highways Administration requires pavement data

from the Colorado Department of Transportation. In this case, they can be considered primary data users. CDOT engineers or planners that use the data may also be primary data users. Changes of data format, type, quality, or products are typically driven by primary data users.

9. Secondary Data User

   Secondary data users are the agencies, persons, or processes that use the data, but are not in the data provider's line-of-business. Secondary users are the entities that rely on production of enterprise data to support their processes, but are outside of the data provider's line-of-business. There is no formal agreement, contract, or mandate that requires the data provider to produce data for this customer. There is no requirement on the data provider to change the data format, type, quality, or products based on the needs of secondary users.

10. Data Provider

    A data provider is a person or organization that functions as the primary custodian and/or owner of a data source made accessible to a wide audience of users. This includes organizations or persons with missions encompassing or requiring enterprise data collection, management, or publication. Data providers should have a lead role in updating and providing enterprise data in an environment and format that can be accessed and used by a larger audience, with proper consideration to sensitivity, legal, and policy concerns that may restrict access and distribution. A enterprise data provider should agree upon a specific level of data quality for the data that is going to be shared, and this level should be maintained unless there is a good reason to deviate from it, and any deviations should also be well documented.

11. Data Owner

    A data owner is a person or organization having the responsibility and authority for an entrusted data resource. Entrusted data is data that is owned by an entity that can authorize or deny access to this data, and is responsible for its accuracy, integrity, and timeliness, and maintenance/production of record level metadata. Policies, procedures, and technical processes for the accuracy, integrity, timeliness, and satisfying standards of metadata should be documented and widely communicated.

12. Primary Content Provider

    A primary content provider is the entity that is primarily responsible for maintaining data available to users. This is the agency that is primarily responsible or has assumed the primary role of maintaining a given data set. An example of this is CDOT for roads. Most of the Primary Content Providers will arise organically based on agency business needs rather than being appointed or mandated to act in this role. Nonetheless as data governance proceeds, the agencies should be explicitly identified as Primary Content Providers.

13. Secondary Content Editor

    A secondary content editor is an entity that adds content, attributes or other relationships, to the data provided by the primary content provider. This is often done for the entities' individual use or needs. However, this function may be included the stewardship process for a data set.

Governance Model

The State of Colorado data stores contain a multitude of various sensitive data, ranging from information to be open sourced (traffic updates) to data that must be carefully guarded (child information). Legislation and regulations exists around much of the data, including Health Insurance Portability and Accountability Act (HIPAA), Family Educational Rights and Privacy Act (FERPA) and a multitude of other legislative regulations and policies around data sharing and governance. Data Stewards will bring their recommendations to the GDAB for approval to ensure validation and verification of rules, as well as ensure the enterprise governance structure remains intact.

In general, there are three questions to ask when creating a governance model around data:

- Who may access the information and why?
- What may they access?
- When may they access the information?

Who May Access and Why

Access to the data should be outlined in a purpose statement, defining why the data is being published.

As appropriate, strict access policies will be placed around data and the governing entity will have complete control over setting and revoking these policies. Three primary rules are defined for Roles Based Access Control (RBAC):

1. Role assignment: A user can exercise a permission only if the user has selected or been assigned a role.

2. Role authorization: A user's active role must be authorized for the user. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.

3. Permission authorization: A user can exercise a permission only if the permission is authorized for the user's active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized

> *In accordance with the state's security policies, users will only be granted the least amount of privileges required to do their work. Other permissions may be required, such as a person who can decide a change in role may not be the same person who can revoke that change.*

What May Be Accessed

The data will be governed by strict policies, as necessary. Following the State's security policy around data classifications, the CIM will provide four levels of governance. (The policy around data classifications may be found here.)

- Unrestricted

  Data may be open sourced and used by both public and private entities without restriction. An example is traffic update information. Aggregate data may also fall into this category.

- Level 1

  Data may be sourced with little regard to integrity or breach, but may require specific access rights for a user. In general, this data is relatively unguarded. An example is a report regarding classroom attendance for each school district that may only be accessed by teachers and education officials. Certain aggregate data may also fall into this category.

- Level 2

  Data must be restricted and accessed only by authorized personnel. No specific legislation or policies prevent access to the data, but loss or breach could amount to disruption of services and distrust of the public. An example is motor vehicle registration information. This data must be protected by RBAC.

- Level 3

  Data must be restricted and there may be significant regulation around it.

  - If the data may be joined with other data to create non-compliance with regulation (such as HIPAA or FERPA), then access to the data may be restricted to aggregated information.
  - If the data itself is restricted in some manner, the data may be accessed in a 'yes/no' way if it meets regulatory standards.
  - Consent of the data may be required at the individual level, as is the case for the Health Information Exchange.
  - Other standards and policies as required.

When Can the Data Be Accessed

Under certain circumstances, data that is restricted may be accessed. For instance, if a child is in danger, their data may be exposed to a case worker requiring certain information for a certain time period.

These types of circumstances will be taken as one-off situations until standards can be placed around them. In general, they will be a combination of RBAC and Level 3 policies.

Data Governance Roles

Director of Information Architecture and GDAB

The Director of Information Architect within the Office of Information Technology and GDAB will be responsible for defining requirements and standards that cross agency/entity boundaries:

- Enterprise Policy Definition
  - HIPAA
    - http://www.colorado.gov/cs/Satellite/DPA-DHR/DHR/1236690495451
  - HIPAA Liaisons by Facility
    - http://www.colorado.gov/cs/Satellite/CDHS-Ops/CBON/1251580657464
  - FERPA
    - http://www.cde.state.co.us/cdereval/Ferpa.htm
  - Privacy
    - Individual Anonymization
    - Aggregate Anonymization
  - Other
- Enterprise Technical Role Definition
  - RBAC Model - The permissions to perform certain operations are assigned to specific roles/job functions.
    - Role assignment: A subject can exercise permission only if the subject has selected or been assigned a role.

        - Role authorization: A subject's active role must be authorized for the subject. With rule 1 above, this rule ensures that users can take on only roles for which they are authorized.
        - Permission authorization: A subject can exercise permission only if the permission is authorized for the subject's active role. With rules 1 and 2, this rule ensures that users can exercise only permissions for which they are authorized.
    - Example roles
        - System Administrator Role
        - Database Administrator Role
        - Data Analyst Role
- Enterprise Security (in conjunction with CISO office)
- Enterprise Access Definition
    - Onboarding
    - Offboarding
    - Redissemination authority
- Enterprise Quality Standards
    - Data Certifications
    - Rating systems
- Enterprise Information Exchanges
    - Reference appendix C and D and http://www.colorado.edu/pba/surveys/nondisclosure.htm
    - Process
    - MOU's
    - Approval Forms
- Enterprise Data Dictionary
    - Reference appendix E

Data Steward Coordinator

Each entity will select data stewards within their organizations who are responsible for the governance and policies around their data. These entities (whether individual, board or other entity type) will address the business policies, procedures, and governance of the information.

The data stewards are responsible for:

- Data Standards: Adherence to established Data Standards or creating and evolving standards if none exist.
- Data Dictionary:
    - Identification of the data elements
    - Information on interpretation of data
    - Information on how the data was collected
- Perform Needs Assessment
    - Identify needs
    - Identify data sources
    - ROI
- Establish and maintain a team to define processes
    - Change management
    - Standards enforcement
    - Establishing decision rights
    - Conflict management

- Perform data compilation and maintenance
  - Collecting data
  - Assuring data quality
- Data Governance:
  - Credibility and quality of the data.
  - Policies and regulations that must be applied
    - HIPAA
    - FERPA
    - Other regulations
  - Publishable data
    - Data Level Definition
    - Aggregate Rules
    - Individual Rules
  - RBAC
    - Roles and permissions
  - Consent Required
- Information Exchange Requirements
  - Security
    - Digital Certificates (required: yes/no)
    - Message Authentication (required: yes/no)
    - Other Security as necessary
  - Publishing Information
  - File Description
  - File Layout
  - Field Definitions

Data Governance Framework – DGI Data Governance Framework™

Business needs drive information needs which drive technology strategies and approaches.

People and Organization (who)

1. Data Stakeholder – an individual or group that could affect or be affected by the data.
   a. Usual suspects IT Teams, Data Architects, DBA's, business groups
2. Data Governance Office
   a. Liaison to data quality, security, architecture, compliance, policy
3. Data Stewards
   a. A person, group , organization delegated the responsibility for managing a specific set of data resources entrusted to them by the data providers and/or owners
   b. Two types
      i. Coordinator (data/system)
         1. Tactical
         2. Track data source to destination
      ii. Corrector
         1. Understand the business rules and policy
         2. Fix data
   c. 5 models - Cross Functional / Hybrid approach is most common
      i. Subject Area (Customer, product, service, geography, time)
      ii. Organization
      iii. Business Process
      iv. Application
      v. Project

Rule and Rules of Engagement (why and what)

1. Data Governance Missions and Visions
2. Focus Areas
    a. Goals, Governance Metrics and Success Measures, and Funding Strategies
    b. Metrics what is success and how do we measure
        i. If we do A, then we should expect B, with a result of C; otherwise, we should expect D, with a result of E.
    c. How you could fund your Data Governance Office (or its equivalent)
        i. How you could fund Data Analyst/Architecture time needed to help define rules, define data, and research issues that must be resolved
        ii. How you could fund Stewardship activities
    d. What protocols need to be established for Business and IT staff who
        i. Help define data
        ii. Analyze data issues
        iii. Help resolve data issues
3. Data Rules and Definitions
    a. data-related policies, standards, compliance requirements, business rules, and data definitions
4. Decision Rights
    a. Who gets to make the decision, and when, and using what process
5. Accountabilities
    a. new paradigm says that, for efforts with a compliance requirement, work is not finished until you
        i. Do it
        ii. Control it
        iii. Document it
        iv. Prove compliance
6. Controls
    a. Preventive
    b. Detective
    c. Corrective
    d. Manual
    e. Technology
    f. Automated

Processes – how is data used, when and by whom

1. Develop a value statement use the A,B,C approach
    a. If we do A, then we can expect B, which should lead to C
2. Prepare a road map
3. Plan and fund
4. Design the program
5. Deploy the program
6. Govern the data
7. Monitor, measure and report

Data Governance Operational Framework

Strategy

1. Strategy and Mission
2. Organization and Planning

Executed by "People"

1. Data Governance Council (who work with)
2. Data Stewards (to serve)

3. Data Stakeholders

Through a set of integrated "Processes"

Meetings and Communication (establishing)

1. Decision Rights and Controls (operated via)
2. Roles and Responsibilities

Ensures accurate "Data" through "Policies"

1. Data Assets (are consistent through)
2. Rules and Standards (driven from)
3. Policies (to ensure)
4. Compliance (and)
5. Data Quality (all of this monitored through)
6. Performance Metrics

Enabled by "Technology"

1. Business Intelligence Applications
2. Data warehouse and integration tools
3. Master Data and Metadata
4. Data Quality Tools

Stewardship Process

A structure for governance of enterprise data includes a standard set of steps for stewarding data sets. This does not imply that a data steward should be responsible for all of these steps, but it does mean that if an agency accepts the responsibility of acting as a steward of a particular data set, it will accomplish at least a subset of these tasks. When this agency accepts the stewardship role, it will identify the level of stewardship it can accomplish by identifying which of the tasks it can complete. In this way, the stakeholders and users of this data set will have a clear idea of how the data is being stewarded, and this idea may be consistent across data sets.

The steps below are categorized into logical groupings. Again, an agency stewarding data should not necessarily pursue all of the steps in each group, but such groups do clarify the process. Some of these steps are administrative in nature while others are technical. The technical steps introduce additional infrastructure resource requirements as well as personnel requirements. The steps may be thought of as increasing levels of maturity in stewarding data from basic coordination types of activities to full data integration. The steps in data stewardship are:

- Perform a needs assessment including identifying needs, data sources, return on investment and clarifying the value of data assets and data
- Establish and maintain a team to define processes for change management, standards enforcement, establishing decision rights, conflict management and pool funding and acquire grants.
- Perform data compilation and maintenance potentially including collecting and centralizing data, assessing the quality of data, compiling data into single data sets and integrating edits to data on an ongoing basis.
- Support data distribution potentially by publishing data to a clearinghouse but also by providing adequate descriptions of the data, its recency and managing risk related to the data.
- Identify data governance policies and standards appropriate for data sets.

These steps do not necessarily have to be pursued sequentially. That is, the last two steps in the list may be performed at any time. However, the first two steps listed should be the first tasks undertaken when engaging in stewardship of a data set.

In actuality, the ongoing process of stewarding data will involve all of these steps in a continuous cycle. That is, the needs for a data set are identified followed by data collection and integration and then ongoing compilation and maintenance of the data.

Need assessment

Identify the need for and status of a data set.

1. Identify Stakeholders – who are the data providers and consumers?
2. Identify needs – identify the business need and business objective for different stakeholders.
3. Identify data sources
4. Calculate investment in data assets and data – total cost for collecting, managing, maintaining, and using the data.

Establish and maintain a team

1. Governance groups
    a. Stakeholders
    b. Data governance group
2. Change Management
3. Standards enforcement
4. Establish decision rights
5. Conflict management
6. Pooled funding and grants

Data Compilation and Maintenance

1. Collect and centralize storage
2. Quality assurance and Quality control or data
3. Compile data into a single data set
4. Integrate edits to data

Distribution

1. Data description
2. Recency of Data
3. Risk management and data security

Data Governance and Standard Process

1. Aligning goals and benefits
2. Collect, choose, review, monitor standards
3. Align policies and standards (bottom up)
4. Implement policies and standards
5. Review, approve and monitor polices

Publishing the Information

The Colorado Information Marketplace will follow the standard set by www.data.gov.

Metadata

Metadata describes the data, where and how it was gathered, and information about whom and how to access it, as well as other pieces of information that may be helpful for an entity attempting to use the information.

First, the data set will be catalogued onto the website and include:

- Type
- Agency (dropdown)
- Level
- Data Dictionary
- Name of Data Set
- Description
- Category (dropdown)
- Keywords (for search)

- Information about data access
    - Web Service
    - Downloadable (with description of format)
- Description
    - Date
    - Type and reason for creation
    - Interpretation
- Permissions
- Data licensing
- Agency
- Sub-agency
- Date Released
    - If web service, then date of service release and versions
- Last Updated
- Time Period
- Frequency of Update
- Type of Restrictions
    - FERPA
    - HIPAA
    - other
- Unit of Analysis
- Granularity
- Coverage
- Collection Mode
- Technical Documentation
- Data Quality Certified
- Privacy and Confidentiality
- Data Quality Guideline Certification Website

Data Set

Downloadable Raw Data

This data is uploaded into the marketplace and may be accessed by parties with the correct access and user rights. This data constitutes a 'point in time' snapshot of the data. The format of the data will be easily accessible by those downloading it and should be one of the following with few exceptions:

- CSV, comma delimited

- Pipe delimited
- XML

Frequencies for updates may be one time, daily, weekly, monthly, yearly, or any timeframe that makes the most sense for the data.

Real Time Access

Critical data may require real time access, such as Healthcare Information. Web Services will be provided to users with access rights to the data. Level 0 and 1 data do not have restrictions.

These services will be provided using industry standards around the services and should conform to the following as closely as possible or use like security and technology:

- Security Assertion Markup Language (SAML) 2.0 and above for authentication for Level 2 and 3 data or other approved industry standard
    - http://saml.xml.org/wiki/saml-introduction
- eXtensible Access Control Markup Language (XACML) for access and policy management as necessary
- SOAP, REST or other industry standard
- Encryption (SSL, HTTPS)

Entities supporting the data should ensure its accuracy.

More information regarding web services can be found in the Enterprise Architecture Roadmap 2011-2014.

Other

Entities may wish to publish their own data and merely use the state's website to catalog the information and give users a one stop shop. Some states have adopted a data store model where they create small data stores with only publishable, relevant data that can be made available to other entities. Others have created web services for access.

Sustainability

The Government Data Advisory Board has proposed a fee based structure for certain types of information. Once this is approved and posted, a link will be included here. This fee will be used to cover basic expenses of standing up the software, maintenance costs and the like.

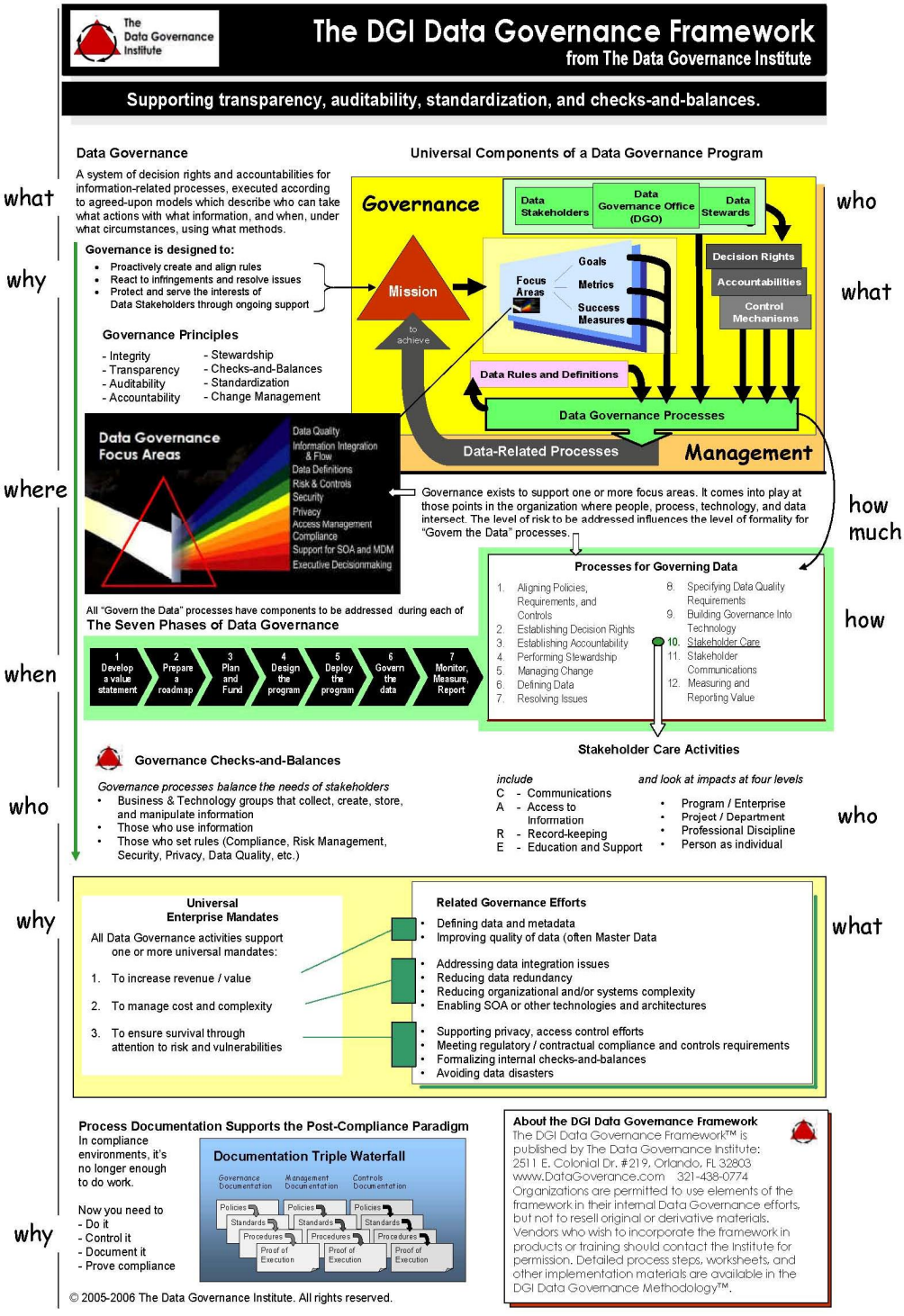
Grants and government incentives will also drive the sustainability model for software and hardware maintenance. However, the CIM will be completely reliant on the participation of various entities to ensure catalogues and data sets are kept up to date.

Conclusion

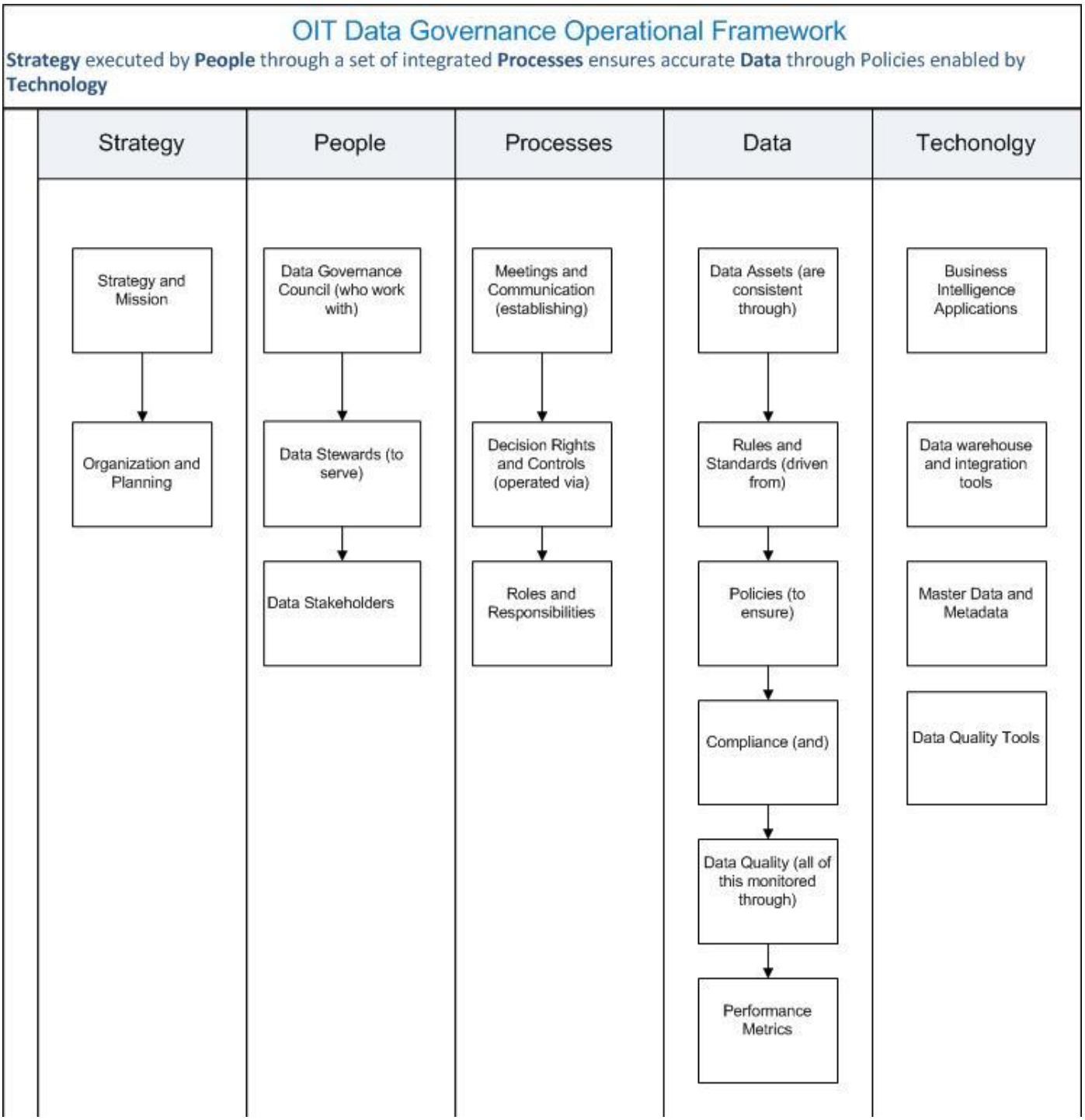
Information sharing and interoperability has become ubiquitous in the private sector over the last few years, with the ability to create new technologies by 'mashing up' data that was previously unavailable and disintegrated. For example, The Huffington Post is essentially a news aggregator, mashing up various blogs and news feeds. Google maps is being used to map everything from real estate availability to urgent care centers and the credit card industry is made up almost entirely of information exchanges. Every day more information is available and being used in creative and innovative ways. Access to information, not just data, creates competitive advantage for any entity looking to improve its services.

The Colorado Information Marketplace is the public sector answer for information exchange and interoperability.

Appendix A: DGI Data Governance Framework™



Appendix B: Data Governance Operational Framework



Appendix C: Sample Data Access and Use Request Form

DEPARTMENT OF EDUCATION

ROUTING SLIP

RESTRICTED DATA USE AGREEMENT

Please review, initial and pass on.

Date:	Please return to: Ph.	Contract #
Name of Research/Analysis Project:		
Director originating this agreement:		

Reviewers:	Initials:	Date:
Director		
Assistant Superintendent		
Deputy Review if checked ☐		
Office of Information Management (final sign off)		

Instructions:

The director originating the research/analysis project should use this form to route the Restricted Data Use Agreement.

Upon receipt of this completed form, the Office of Information Technology will sign the agreement on behalf of the Department of Education, returning the original agreement to the originating director.

Ad Hoc Review Committee – An ad hoc committee should be formed to review the research/analysis project that is proposed in the agreement. List members of the committee below.

Rev. November 2011

Restricted-Use Data

"Restricted-Use Data is personally identifiable information requiring specific procedures to protect confidentiality.

"Public-Use Data" is data that contain no personally identifiable information requiring no specific procedures to protect confidentiality. "Merging Restricted-Use data records with Public-Use data records" means a file containing both Restricted-Use Data and Public-Use Data merged into one file or report. This file or report is considered Restricted-Use Data. Merely deleting identifying fields from a "Restricted-Use Data" file *does not* create a "Public-Use Data" file. Disaggregations of "Restricted-Use Data", even without explicit identification fields, may result in a record where the identity of the subject could be reasonably inferred.

A "Restricted Data Use Agreement" between the Department of Education and any contractor receiving Restricted-Use Data must be completed and signed by all parties prior to transferring any restricted-use data out of the agency.

The Family Education and Right to Privacy Act, Virginia's Government Data Collection and Dissemination and Practices Act, and other regulations may place further restrictions on the dissemination of restricted-use data.

Sample Data Use Agreement

The Data User can sign and complete this data use agreement when submitting a request (application) for confidential data.

A program should amend this template prior to use in the following areas:

a. First paragraph, insert *Agency/Program/Division/Data Owner*.
b. In section *g, Public Release*, insert any program or divisional requirements related to aggregating data for public release.
c. In section *m: Publication*, insert any requirements for disclaimers, credits, authorship, etc.
d. Designate a confidentiality agreement for the user to sign. It is the responsibility of the data user to have additional individuals sign the agreement if more are added during the course of the work. This is Attachment B.

If the program decides to release confidential information, but not the information as requested in the application, a note of what is actually released is should be included in the blank under **Program Name** obligations.

Data user should explicitly indicate any follow-back that is proposed in section *c*.

Data Use Agreement

This Data Use Agreement (Agreement) is between the *Agency/Program/Division/Data Owner*, referred to as **Program Name** and _____ located at _____, referred to as **Data User**.

Program Name Obligations:

Program Name will agree to provide the following information to the Data User in the format as indicated in the Application or alternatively: (list files, by source, with data elements, and the format data is to be delivered in, and note if paper files, computerized records, etc. if different than that requested in the Application.)

_____

_____

Data User Obligations:

a. *Uses and disclosures as provided in this agreement.* Data User may use and disclose the confidential information provided by **Program Name** only for the activity described in the Application. 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 Application.

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 applicable law.

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 (indicate Not applicable if no follow-back is proposed): _____
_____

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. The Data Owner must ensure that no identifying information will be transmitted through unsecured telecommunications, including the unsecured Internet connections.

e. *Confidentiality Agreements.* Data User will ensure that all persons who have access to the confidential information sign the confidentiality agreement, **Attachment B**. This includes, but is not limited to all interns, sub-contractors, staff, other workforce members, and consultants. A copy of the signed confidentiality agreements shall be maintained on file and be available for review by **Program Name** if requested.

f. *Reporting.* Data User shall report to the **Program Name** 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. Furthermore, any reports or aggregate tabulations that are prepared must: (*insert program or divisional requirements for publications if any or remove this sentence.)*

h. *Destruction of Records at End of Activity.* Records, along with any and all copies, must be destroyed in a secure manner or returned to **Program Name** at the end of work described in the Application. Data User agrees to send a written certificate that the data, along with any and all copies, have been properly destroyed or returned within 30 days of the end of the work as described in the Application or: _____, 200_.

i. *Minimum Necessary.* Data User attests that the confidential information requested represents the minimum necessary information for the work as described in the Application and that only individuals with a need to know will have access to the confidential information in order to perform the work.

j. *Institutional Review Board (IRB).* If the Activity involves research, the Data User agrees to furnish all documentation concerning IRB reviews, and to submit required documentation to an IRB or Privacy Board should research protocols change. Data User agrees to submit to **Program Name** any change in waiver status or conditions for approval of the project by an IRB relating to the work described in the Application.

k. *Authorizations.* Data User agrees to secure individual authorizations to use the confidential information if the Activity is research unless an IRB has approved a waiver of an authorization. Documentation must be provided prior to receipt of the confidential information. Research means a systematic investigation designed to develop or contribute to generalizable knowledge

l. *Data Ownership.* The **Program Name** is the data owner. The Data User does not obtain any right, title, or interest in any of the data furnished by the **Program Name**.

m. *Publication/release requirements.* Any release of information must include the following statement: (*insert program or divisional requirements for publications*) In addition, Data User will notify **Program Name** when the publication or presentation is available and provide a copy upon request.

Signed by Program Name: _____Date:_____

Signed by the Data User: _____ Date:_____

Appendix D: Sample Data Privacy Checklist

Data Privacy Checklist

☐	The type of data to be collected has been identified and documented	
	☐	The format in which the data is to be collected has been identified and documented
	☐	The manner in which the data is to be collected has been identified and documented
☐	The rationale/reasoning for the collection of the data has been identified and documented	
☐	The intended use of the data to be collected has been identified and documented	
☐	The entities that may make use of the data to be collected have been identified and documented	
☐	The opportunities that individuals from whom the data is to be collected have to decline to provide data have been identified and documented	
☐	The opportunities that individuals from whom the data is to be collected have to rescind previously granted permission to collect, store, use, and/or transmit data have been identified and documented	
☐	The manner in which the data to be collected will be secured has been identified and documented	
	☐	Secure collection mechanisms have been identified and documented
	☐	Secure storage mechanisms have been identified and documented
	☐	Secure usage mechanisms have been identified and documented
	☐	Secure transmission mechanisms have been identified and documented
	☐	Secure disposal mechanisms have been identified and documented
☐	A system of records pertaining to the data to be collected has been identified and documented	

Document any exceptions and/or waivers to the above items:

Appendix E: Sample Entity Data Privacy Checklist

Entity Data Privacy Checklist

☐	We have a comprehensive set of Data Security Policies	
	☐	Our Policies include technical, administrative, and physical controls to safeguard Private Data
	☐	Our Policies specify the circumstances and manner in which Private Data can be captured, stored, accessed, and/or transported/transmitted
	☐	Our Policies specify the provision of regular and ongoing employee training in the handling of Private Data
	☐	Our Policies specify the process for monitoring employee compliance, and the disciplinary measures for policy violation
	☐	Our Policies include provisions for the monitoring of applicability/effectiveness in regards to the protection of Private Data
	☐	We have designated an individual to oversee the implementation and maintenance of our Policies
☐	We have identified all stores of records that contain Private Data	
☐	We only collect Private Data that is sufficient to meet our legitimate business purposes	
☐	We only retain Private Data for a period of time that is sufficient to meet our legitimate business purposes	
☐	We restrict access to Private Data to only those individuals that have a need to know that is defined by our legitimate business purposes	
☐	We have identified and evaluated reasonably foreseeable internal and external risks to all records containing Private Data	
☐	We have implemented appropriate physical controls to protect Private Data	
	☐	We store all physical copies of Private Data in locked and access controlled facilities and in locked cabinets/storage containers within those facilities
	☐	We house information systems that capture, store, access, or transmit Private Data in locked and access controlled facilities and, where possible, within locked cabinets/storage containers within those facilities
	☐	We use access control mechanisms that restrict physical access to Private Data or information systems that house Private Data to only those that have a business reason for accessing that information
	☐	We require all visitors to facilities that house physical copies of Private Data or information systems that capture, store, access, or transmit Private Data to be positively identified prior to admittance and be escorted at all times after admittance
☐	We have implemented appropriate electronic safeguards to protect Private Data	
	☐	We use and keep patched network firewalls and endpoint firewalls on endpoints that capture, store, access, or transmit Private Data

Appendix F: Sample Data Sharing Agreement

Data sharing agreement

A Data Sharing Agreement DSA) is an enforceable agreement that documents obligations and permissions of, and prohibitions on, collaborating parties when sharing data. The collection of obligations, permissions and prohibitions is usually captured in the clauses of the DSA. DSAs are agreements among distributed entities, speaking about data and representing data policies being communicated among different parties.

The general template structure of agreements and the twenty-one issues addressed – individual agreements may not address all these issues, but only the appropriate subset.

1. Definitions: Terms used in the agreement such as personal data and computing terminology are defined.
2. Parties to the agreement: Definition of the parties making the agreement.
3. Purpose of the agreement: The purpose of the required data sharing in layman's language. Any specific statutory citations should be included.
4. Period of agreement: The time period during which the data sharing agreement shall apply.
5. Justification for access: Details of why general data sharing or data confidentiality principles are being breached by this agreement.
6. Description of the data: Detailed information on which data sets will be cover by the DSA. Does the provider retain ownership?
7. Data Quality: It should make a statement on the degree of commitment to data quality. It could say, for example how the parties are to maintain the quality of the data. Alternatively, it may make a statement that limits liability on the data being accurate, up to date, or reliable.
8. Description of the data users: Statement of who can access and use the shared data. This may be stated in terms of general roles, or specifically by naming individuals.
9. Method of data access or transfer: This section may contain specific details such as, information on the type of encryption to be used, a description of the trusted computing infrastructures that may be used, a description of the trust domains, requirements for physical security, strength of passwords and other security concerns related to data access and transfer.
10. Location of data and custodial responsibility: Description of who is responsible for the data and therefore responsible for the confidentiality requirement stated below.
11. Trustworthiness: This section constrains how much of the infrastructure (hardware, software, network channel etc.) or platform is trusted, e.g., whether a trusted computing platform must be used, users are not permitted to have administrative rights, whether certain hardware and software are to be used. It exports controls on the data.
12. Data use: Statement on how the data can or cannot be used. The use of the data can be defined through a formal document. Refer to sample Data Use Agreements.
13. The position of the agreement with respect to derived data. It may describe who is responsible for the derived data and what policies are to be applied to them
14. Dissemination to third parties: These policies may be included in other sections, but address different classes of data and how data can be disseminated to third parties.
15. Confidentiality: The user agrees to establish appropriate administrative, technical and physical safeguards to ensure the confidentiality of the data and to prevent unauthorized

use, disclosure or access to it. The details in this section can be as general as the previous statement, or as detailed as possible depending on the style of agreement.
16. Disposition of data: The policy for disposing of data at the termination, or expiration, of the agreement or as per applicable law.
17. Administration of the Agreement: Process for reviewing and updating the agreement who, how often etc. Procedure for terminating, and perhaps renewing the agreement.
18. Breaches to the agreement: Define the procedure to record breaches and the action to be taken on breaches.
19. Applicable law: The law which applies to the agreement, or a clear statement that the agreement does not constitute a contract which is enforceable in any jurisdiction.
20. Financial: Any costs associated with sharing the data should be noted, along with the manner of reimbursement.
21. Signature: Authorized parties confirming the agreement.

Appendix G: Sample Data Policy

Title: **Data Privacy Policy**	Document ID:	P-
	Creation Date:	June 24, 2011
	Revision Date:	
	Version:	1.0

TITLE: DATA PRIVACY POLICY

1. **PURPOSE:**

   The purpose of this data privacy policy is to promote greater access to data for better decision-making, decreasing redundancy and promoting efficiency between governmental entities as well as external entities interacting with governmental entities, while ensuring the confidentiality, integrity and availability of data.

2. **POLICY:**

   State agencies shall ensure the confidentiality, integrity and availability of the data that they gather or collect, receive, maintain, store, access, disclose, or disseminate to a political subdivision or to a nongovernmental entity or an individual. This shall be through, but not limited to, the establishment of appropriate policies and/or procedures. These policies and/or procedures shall ensure the legal, appropriate and ethical sharing of data per applicable federal, state, local and tribal law. The established policies and/or procedures, at a minimum, must address the requirements as stated in Section 6.

3. **ORGANIZATIONS AFFECTED**

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

4. **REFERENCES**

   4.1. "Office of Information Technology, Definitions", C.R.S. 24-37.5-102, "Office of Information Technology, Interdepartmental Data Protocol", C.R.S. 24-37.5-7

   4.2. Privacy Act of 1974

   4.3. "Health Insurance Portability and Accountability Act of 1996", 42 U.S.C. sec. 1320d to 1320d-9

   4.4. "Family Educational Rights and Privacy Act of 1974", 20 U.S.C. sec. 1232g

   4.5. "Confidentiality of Alcohol and Drug Abuse Patient Records", CFR Title 42, Part 2

   4.6. NIST SP800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)

   4.7. Global Justice Information Sharing Initiative, "Privacy and Civil Liberties Policy Development Guide and Implementation Templates

   4.8. Governor's Office of Information Technology, "Guidelines for Information Sharing"

Title: **Data Privacy Policy**	Document ID:	P-
	Creation Date:	June 24, 2011
	Revision Date:	
	Version:	1.0

4.9. Governor's Office of Information Technology, "Data Retention and Destruction Policy Template"

4.10. Governor's Office of Information Technology, "Data Sharing Agreement Template"

4.11. Governor's Office of Information Technology, "Data Usage Policy Template"

4.12. Governor's Office of Information Technology, "Information Quality Guidelines"

4.13. Governor's Office of Information Technology, "Entity Data Privacy Checklist"

4.14. Governor's Office of Information Technology, "Data Privacy Checklist"

5. DEFINITIONS

5.1. The term "privacy" refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data.

5.2. Personally Identifiable Information (PII) is —any information about an individual maintained by an entity, including (1) any information 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 (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

5.3. Protected Health Information (PHI) under HIPAA includes any *individually identifiable* health information. *Identifiable* refers not only to data that is explicitly linked to a particular individual (that is *identified* information). It also includes health information with data items which reasonably could be expected to allow individual identification.

5.4. "Interdepartmental data protocol" means an interoperable, cross-departmental data management system and file sharing procedure that permits the merging of unit records for the purposes of policy analysis and determination of program effectiveness. The Interdepartmental data protocol at a minimum shall include protocols and procedures to be used by state agencies in data processing, including but not limited to collecting, storing, manipulating, sharing, retrieving, and releasing data.

6. REQUIREMENTS

The established policies and/or procedures, at a minimum, must address:

6.1. That all practicable measures to ensure personal privacy and protect personal information from intentional or accidental release to unauthorized persons and from intentional or accidental use for unauthorized purposes have been taken

6.2. That the Interdepartmental data protocol is implemented and followed

6.3. That the appropriate Data Sharing Agreements will be put in place for all data sharing initiatives

6.4. Identification of applicable federal, state, local, and tribal law

Title: **Data Privacy Policy**	Document ID:	P-
	Creation Date:	June 24, 2011
	Revision Date:	
	Version:	1.0

6.5. Who is responsible for the enforcement of the policies and/or procedures

7. RESPONSIBILITIES

Agency Executive Management is responsible for:

7.1. Ensuring that this policy has been implemented and is being enforced.

State Chief Information Security Office is responsible for:

7.2. Coordinating a periodic audit of the policies and/or procedures.

8. COMPLIANCE

8.1. All entities identified in Section 3 of this policy are required to comply with this policy.

9. EXPIRATION

9.1. This Policy will remain in effect until the State CIO revises, changes or terminates it.

Appendix H: Sample Interagency Agreement

Routing # CMS #

STATE OF COLORADO
LIEUTENANT GOVERNOR'S OFFICE
EARLY CHILDHOOD LEADERSHIP COMMISSION
INTERAGENCY AGREEMENT
with
GOVERNOR'S OFFICE OF INFORMATION TECHNOLOGY

TABLE OF CONTENTS

1. PARTIES
This Interagency Agreement (hereinafter called "Agreement") is entered into by and between the Lieutenant Governor's Office, Early Childhood Leadership Commission (hereinafter called "ECLC"), and the Governor's Office of Information Technology (hereinafter called "OIT"), 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 AND NOTICE OF NONLIABILITY.
This Agreement shall not be effective or enforceable until it is approved and signed by the Colorado State Controller or designee (hereinafter called the "Effective Date"), but shall be effective and enforceable thereafter in accordance with its provisions.

3. RECITALS

A. Authority, Appropriation, And Approval
Authority to enter into this Agreement exists in an appropriation made to fulfill the objectives outlined in Colorado's 2009 ARRA Early Childhood Leadership Commission/ Head Start State Advisory federal grant award; specifically the measurable objectives described in ECLC grant application. The award period for this funding is July 1, 2010 –May 31, 2013. The DUNS number for this award is 188589402. CFDA number is 93.708. PR/Award number 90SC0006. For more information on the SLDS grant, refer to the project website at www.cde.state.co.us\SLDS, and funds have been budgeted, appropriated and otherwise made available and a sufficient unencumbered balance thereof remains available for payment. Required approvals, clearance and coordination have been accomplished from and with appropriate agencies.

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
OIT shall provide business or technology systems resource(s) for the purpose of surveying the needs, interests, and gaps in technology of Colorado's Early Childhood Programs and provide IT expertise and make recommendations to the ECLC for designing and implementing a data system for early childhood

data management as per OIT and the GDAB Guidelines for Information Sharing. OIT will work with the ECLC and the Executive Directors of the partnering departments to provide recommendations and a governance process framework for the ECLC to design and implement the infrastructure desired in the Early Childhood Data System they seek to build upon securing funding required to do so.

D. Termination of Previous Contract

Whereas the Parties executed Agreement CMS # 30927 effective February 1, 2011 and pursuant to Section IV.A, of that Agreement now terminate that Agreement and replace it with this Agreement.

4. TERM AND EARLY TERMINATION

A. Term-Work Commencement

The Parties respective performances under this Agreement shall commence on the Effective Date. This Agreement shall terminate on May 31, 2013 unless sooner terminated or further extended as specified elsewhere herein. Either Party may terminate this Agreement by giving the other Party 30 days prior written notice setting forth the date of termination. Upon termination the liabilities of the Parties for future performance hereunder shall cease, but the Parties shall perform their respective obligations up to the date of termination.

5. STATEMENT OF WORK

A. Work

OIT shall complete the Work and its other obligations as described herein and in **Exhibit A** on or before May 31, 2013. The ECLC shall not be liable to compensate OIT for any Work performed prior to the Effective Date or after the termination of this Agreement.

B. Goods and Services

OIT shall procure goods and services necessary to complete its obligations. Such procurement shall be accomplished using Agreement Funds and shall not increase the maximum amount payable hereunder by the ECLC.

6. PAYMENTS-MAXIUM AMOUNT

The maximum amount payable under this Agreement to OIT by ECLC is $100,000.00, as determined by ECLC from available funds. Payments to OIT are limited to the unpaid obligated balance of this Agreement set forth herein. ECLC shall make payment for purchases of goods and services within 30 days after receipt of valid invoices from OIT. Payments shall be made by an interagency transfer in lieu of a State warrant whenever possible. The maximum amount payable by ECLC to OIT during each State fiscal year of this Agreement shall be:

$ 40,000.00 in FY12
$ 60,000.00 in FY13

An explanation of the goods and/or services purchased by OIT must accompany each payment request from OIT which includes detail of how the purchase meets specific measureable objectives of the ECLC project. All requests for reimbursement from OIT must be accompanied in a format to be provided to OIT by ECLC that includes all information necessary for ECLC to comply with the subrecipient reporting requirements of the American Recovery and Reinvestment Act (ARRA).

7. RECORDS-MAINTENANCE AND INSPECTION

A. Maintenance

During the term of this Agreement and for a period terminating upon the later of **(i)** the five year anniversary of the final payment under this Agreement or **(ii)** the resolution of any pending Agreement matters (the "Record Retention Period"), each Party shall maintain, and allow inspection and monitoring by the other Party, and any other duly authorized agent of a governmental agency, of a complete file of all records, documents, communications, notes and other written materials, electronic media files, and communications, pertaining in any manner to the work or the delivery of services or goods hereunder.

B. Inspection

The ECLC shall have the right to inspect OIT's performance at all reasonable times and places during the term of this Agreement. OIT shall permit the ECLC, and any other duly authorized agent of a governmental

agency having jurisdiction to monitor all activities conducted pursuant to this Agreement, to audit, inspect, examine, excerpt, copy and/or transcribe OIT's records related to this Agreement during the Record Retention Period to assure compliance with the terms hereof or to evaluate performance hereunder. Monitoring activities controlled by the ECLC shall not unduly interfere with OIT's performance hereunder.

8. CONFIDENTIAL INFORMATION-STATE RECORDS

Each Party shall treat the confidential information of the other Party with the same degree of care and protection it affords to its own confidential information, unless a different standard is set forth in this Agreement. Each Party shall notify the other Party immediately if it receives a request or demand from a third party for records or information of the other Party.

9. FAILURE TO PERFORM-DISPUTES

The failure of a Party to perform its respective obligations in accordance with the provisions of this Agreement is a breach of this Agreement. 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 this fails, the matter shall be submitted in writing by both Parties to the State Controller, whose decision shall be final.

10. NOTICE AND REPRESENTATIVES

Each individual identified below is the principal representative of the designating Party. All notices required to be given hereunder shall be hand delivered with receipt required or sent by certified or registered mail to such Party's principal representative at the address set forth below. In addition to, but not in lieu of a hard-copy notice, notice also may be sent by e-mail to the e-mail addresses, if any, set forth below. Either Party may from time to time designate by written notice substitute addresses or persons to whom such notices shall be sent. Unless otherwise provided herein, all notices shall be effective upon receipt.

OIT
Sherri Hammons
Office of Information Technology
601 E. 18th Avenue, Suite 250
Denver, CO 80203
OITContracts@state.co.us

ECLC
Jennifer Stedron
Office of Lt. Governor Joseph A. Garcia
130 State Capitol
Denver, CO 80203
jennifer.stedron@state.co.us

11. GENERAL PROVISIONS

A. Assignment

The rights and obligations of each Party hereunder are personal to such Party and may not be transferred, assigned or subcontracted without the prior, written consent of the other Party.

B. Order of Precedence

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: The Agreement then the Exhibits.

C. 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.

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.

Routing # CMS #

12. SIGNATURE PAGE

THE PARTIES HERETO HAVE EXECUTED THIS INTERAGENCY AGREEMENT

*** Persons signing for Parties hereby swear and affirm that they are authorized to act on behalf of their respective Party and acknowledge that the other Party is relying on their representations to that effect.**

STATE OF COLORADO John W. Hickenlooper, Governor	
Governor's Office of Information Technology Kristin Russell, Secretary of Technology and Chief Information Officer _____ Signature By: Todd Olson, Chief Financial Officer Date: _____	Early Childhood Leadership Commission Andrew Freedman, Chief of Staff to Lt. Governor Joseph A. Garcia _____ Signature By: Andrew Freedman, Chief of Staff to Lt. Governor Joseph A. Garcia Date: _____

ALL CONTRACTS REQUIRE APPROVAL BY THE STATE CONTROLLER

STATE CONTROLLER
David J. McDermott, CPA

By: _____

Date: _____

EXHIBIT A-STATEMENT OF WORK

The Lt. Governor's Office and the ECLC will partner with OIT and the Government Data Advisory Board (GDAB) on the planning, requirements definition, and data sharing prioritization that will be required to develop a plan and set of recommendations to the ECLC for how they may implement an interagency early childhood data system (EC Data System). OIT has been designated via legislation to oversee and govern all policies, processes, standards and architecture related to enterprise information sharing initiatives. Senate Bill 08-155, the IT Consolidation bill, puts control of all information systems, resources and budget under OIT's control. OIT will draft an EC Data System implementation plan for a unified EC Data System that measures progress and informs planning, policy development and funding of early childhood supports, services and infrastructure. ECLC will review and approve the implementation plan. OIT's delivery of the implementation plan is contingent upon ECLC providing OIT with the requirements, data definitions, priorities and deliverable timelines required by the ECLC grant.

The creation of the EC Data System implementation plan shall include the following measurable outcomes in accordance with the ECLC grant application:

1. Design technical requirements of the ECLC's key questions to be answered based on definitions and priorities set by ECLC;
2. Inventory systems, data and infrastructure of participating agencies' systems; contingent upon ECLC delivery of the questions/requirements requirements and definitions of what data is required to answer the requirements;
3. Explore integration of relevant data sets per ECLC priorities;
4. Perform gap analysis of existing versus needed data based on data definitions set by ECLC;
5. Determine strategy, methods, or recommendations for how ECLC may capture, link, or provide missing data elements;
6. Make recommendations to ECLC regarding regulatory and compliancy review to ensure privacy and confidentiality of data residing in the EC Data System;
7. Ensure alignment and compliance with State enterprise architecture and data management standards, policies, and guidelines to complete the planning for the EC Data System.

Appendix I: Sample Memorandum of Understanding Agreement

Department or Agency Name

Governor's Office of Information Technology
Department or Agency Number

EGB

Contract Routing Number

MEMORANDUM OF UNDERSTANDING

Between

Governor's Office of Information Technology
Communication Services
and

Ramrod Inc. Doing Business as Arkansas Valley Ambulance

For

A Shared Communications Building and Microwave Radio Infrastructure

1. Memorandum of Understanding

This Memorandum of Understanding (MOU) is entered into by and among Ramrod Inc, dba Arkansas Valley Ambulance, P.O. Box 210 Cotopaxi, Colorado 81223, herein after referred to as "AVA", the State Of Colorado, Governor's Office of Information Technology, Communication Services, 601 East 18th Avenue, Denver, CO 80203, herein after referred to as the "State " or "OIT".

2. Purpose

The State and AVA have entered into this MOU to set a framework to allow the State and AVA to share communication sites for the support of public safety communications in the state of Colorado.

AVA is expanding its current VHF radio system to provide public safety base radio communications from the Coaldale remote radio site in Freemont County, and wire line control to Salida dispatch.

3. Statement of Mutual Interests and Benefits

The State provides a public safety communications capability serving state agencies and participating local government entities. As part of this responsibility , AVA is seeking to improve public safety communications in its area of operations.

This MOU is designed to establish a cooperative relationship in the operation of a communication site. The sharing of communications facilities are actions that may substantially reduce costs and enhance interoperable communications for State, County and local public safety providers.

4. Cooperators Agree

4.1 Each party shall be responsible for engineering, providing, installing, operating, and maintaining the necessary equipment within its own system except as specified in Exhibit A, attached to this MOU and incorporated herein by reference.

1

4.2 Unless specifically authorized, no party or representative shall adjust, maintain or otherwise touch equipment owned by another.

4.3 All parties will manage frequencies assigned to them in accordance with FCC regulations. Copies of FCC licenses shall be provided to the site manager, as noted in attached exhibits, upon request. Any party causing radio frequency interference will be responsible for resolving and repairing any and all radio interference issues within a timely and respectful manner by the party causing the interference.

4.4 Parties shall coordinate to provide needed capacity in the form of facilities, antenna space, etc.

4.5 Each party shall follow safety and security guidelines for site user and representatives when accessing the site.

4.6 Each party shall notify the other party 24 hours in advance, if possible, should it become necessary to temporarily sever an interconnection or to interrupt a circuit elsewhere in its system that would affect the operation of the other party's equipment or circuits.

4.7 To the extent authorized by 24-30-1510 (3) (e) CRS, each party shall be liable for losses arising from personal injury, death or property damage caused by the negligent or wrongful act or omission of it employees in accordance with the Colorado Government Immunity Act, §24-10-101 et seq., C.R.S.

5. Non- Fund Obligation Document

This instrument is neither a fiscal nor a funds obligation document. Any endeavor involving reimbursement or contribution of funds between parties will be outlined in separate agreements.

6. No Third Party Beneficiary Rights

Except as otherwise stated, this MOU shall inure to the benefit of and be binding only upon the parties hereto and their respective successors and assigns. No third party beneficiary rights or benefits of any kind are expressly or impliedly provided herein.

7. Terms of Agreement

This MOU will become effective upon receipt of the last signature and will remain in force for 5 years or until terminated by mutual agreement by both parties upon one hundred and eighty days written notice to the others of the intent to terminate. Any participant may propose changes to this MOU during its term. Such changes will be in the form of an amendment and will become effective upon signature by all participants.

8. Authorized Representatives Of The Parties

8.1 Each party shall, by written notice to the other, designate the representative who is authorized to act on its behalf with respect to those matters contained herein that are the functions and responsibilities of the authorized representatives of the parties. Any party may change the designation of its authorized representative upon oral notice given to the other, confirmed promptly by written notice.

8.2 The parties' authorized representatives shall meet at least on an annual basis, and more often as the need arises. The authorized representatives shall address matters of common concern of the parties, and shall review and approve the sharing of extraordinary costs. A simple majority shall grant approvals.

9. Insurance

AVA shall at its sole cost and expense, obtain insurance on its inventory, equipment, and all other property associated with this equipment against loss resulting from fire or other casualty.

10. Control and Possession Of Systems

Each party shall remain in exclusive control and possession of its own telecommunications system and equipment and this MOU shall not be construed to grant any party any rights of ownership, control, or possession of the other party's systems or equipment, other than those which may be specifically set forth herein or in exhibits hereto.

11. Nondedication of Equipment

The parties do not intend to dedicate, and nothing in this MOU shall be construed as constituting a dedication by any party of its rights, or equipment, or any part thereof, to the other party or any customer or member of the other party.

12. Uncontrollable Forces.

No party shall be considered to be in default in performance of any of its obligations under this MOU when a failure of performance shall be due to an uncontrollable force. The term "uncontrollable force" means any cause beyond the control of the party affected including, but not restricted to, failure or threat of failure of facilities, flood, earthquake, storm, fire, lightning, epidemic, war, riot, civil disturbance or disobedience, labor dispute, labor or material shortage, sabotage, restraint by court order or public authority or action or nonaction by, or failure to obtain the necessary authorizations or approvals from, any governmental agency or authority, which by exercise of due diligence and foresight such party could not reasonably have been expected to avoid and which by exercise of due diligence it shall be unable to overcome. Nothing contained herein shall be construed to require a party to settle any strike or labor dispute in which it is involved. Any party rendered unable to fulfill any obligation under this MOU by reason of uncontrollable force shall give prompt written notice of such fact to the other party and shall exercise due diligence to remove such inability with all reasonable dispatch.

13. Notices

13.1Any notice, demand or request pursuant to this MOU herein shall be in writing and shall be considered properly given when delivered in person, sent by either registered or certified mail, or sent by national overnight delivery service, postage prepaid addressed to the other party's principal offices.

13.2 Notices to the State shall be sent to: State of Colorado, Governor's Office of Information Technology, Communication Services, 601 E. 18th Avenue, Suite 250, Denver, CO 80203.

13.3 Notices to AVA shall be sent to: Arkansas Valley Ambulance P.O. Box 210 Cotopaxi, CO 81223.

14. Waivers

Any waiver at any time by a party to this MOU of its rights with respect to a default or any other matter arising under or in connection with this MOU shall not be deemed to be a waiver with respect to any subsequent default or matter.

15. Binding Obligations

All of the obligations set forth in this MOU shall bind the parties and their successors and assigns, and such obligations shall run with the parties' rights, titles, interests, and with all of the interests of each party to this MOU.

16. Effect Of Section Headings

Section heading titles appearing in this MOU are inserted for convenience only and shall not be construed as interpretations of text.

17. Governing Law

This MOU shall be construed and interpreted in accordance with the laws of the State of Colorado.

THE PARTIES HERETO HAVE EXECUTED THIS MEMORANDUM OF UNDERSTANDING

RAMROD INC. d/b/a
ARKANSAS VALLEY AMBULANCE

By_____
Signature of Authorized Officer

Date_____

_____
Print Name & Title of Authorized Officer

STATE OF COLORADO
GOVERNOR'S OFFICE OF
INFORMATION TECHNOLOGY

By_____
Signature of Authorized Officer

Date_____

_____
Print Name & Title of Authorized Officer

Exhibit A

COALDALE COMMUNICATION SITE

At the COALDALE site the AVA shall:

1. License with the FCC the VHF base radio on AVA frequency.
2. Coordinate equipment repair/replacement parts and upgrades with the State.
3. Install and operate their public safety base radio equipment consistent with room configuration plan and consistent with federal and industry standards including current R56 rules. Be responsible for their own equipment repair and maintenance.
4. Prior to any install, there shall be an IM (Intermod) study performed and the results supplied to the State.
5. No one shall be permitted to climb State towers, unless climbers provide current and valid tower climbing and rescue certification and adequate insurance coverage for personnel to climb towers.

At the COALDALE site the State shall:

1. Provide space in the State owned building for all necessary public safety radio equipment.
2. Maintain building, tower, and air conditioning equipment.
3. As site manager, manage the site and approve new users and/or equipment on the site.
4. Provide electrical power to the base radio and associated equipment.
5. Provide and maintain electric backup generator to sustain equipment in the event of a commercial power outage and provide fuel for generator.
6. Provide tower work if no other party is certified and uninsured.
7. Provide electrical service to equipment rack.
8. Provide access to the site.
9. As site manager, approve all equipment installations, configurations, modifications, and layouts of the building and on the tower.
10. Provide installation procedures and designate locations for installation of equipment on the tower.
11. Advise AVA of any proposed changes in the State's lease with the BLM (Bureau of Land Management) that could impair AVA's ability to operate its equipment or meet its operational objectives of the site.

Appendix J: Sample Data Dictionary

Table Name - Citizen					
Column Name	**Description**	**Data Type**	**Length**	**Null**	**Derived**
Social Security Number	**Definition:** nine-digit number issued to U.S. citizens, permanent residents, and temporary (working) residents under section 205(c)(2) of the Social Security Act, codified as 42 U.S.C. § 405(c)(2). **Codes/Notes:** 999999999 **Missing Value:** Does not apply; field must be completed. **Edit Specs:**	Numeric	9	N	N
First Name	**Definition:** character field that is pertaining to one's first, or given name, **Codes/Notes:** none **Missing Value:** Does not apply; field must be completed. **Edit Specs:**	Alphanumeric	50	N	N
Last Name	**Definition:** character field that is pertaining to one's last or surname **Codes/Notes:** none **Missing Value:** Does not apply; field must be completed. **Edit Specs:**	Alphanumeric	100	N	N
Middle Name	**Definition:** the part of a person's name occurring between the first and surnames, as a second given name or a maternal surname **Codes/Notes:** none **Missing Value:** Does not apply; field must be completed.	Alphanumeric	50	Y	N
Date of Birth	**Definition:** The date of birth as designated on the individual's legal birth registration or certificate.	Numeric	8		N

	Codes/Notes: YYYYMMDD YYYY = four-digit year of birth MM = two-digit month of birth DD = two-digit day of birth This field is used to compute a student's age. The Commission computes a student's age for students enrolled in the summer and fall terms as of September 15, and for those enrolled in the winter and spring terms as of February 15. If the student is born on either September 15 or February 15, age is determined by subtracting the year of birth from the report year. Any birth dates before the 15th are calculated by subtracting the year of birth from the report year. Any birth dates after the 15th are calculated by subtracting the year of birth from the report year and then subtracting 1 from that difference. **Missing Value:** Blank, if unknown. **Edit Specs:** Error if computed age is negative or if >110 Warning if computed age is < 14 or > 90 **Updates:** Expanded to four-digit format, year 2000 file conversions, September 1998.				
Ethnicity	**Definition:** The race/ethnic group to which an individual appears to belong, identifies with, or is regarded in the community as belonging. In addition, non-resident aliens, i.e., those members of the aforementioned groups who have not been admitted to the United States for permanent residence, should be separately identified as a sixth category; the non-resident aliens are not separately requested by racial/ethnic group.' THIS FIELD WILL BE PHASED OUT IN FALL 2010 - ONLY BLANKS WILL BE	Numeric	1		N

	ACCEPTED **Codes/Notes:** 1 - Non-Resident Alien 2 - Black, non-Hispanic 3 - American Indian or Alaskan Native 4 - Asian or Pacific Islander 5 - Hispanic 6 - White, non-Hispanic **Missing Value:** Blank, if unknown. **Edit Specs:** Error if > 6. **Updates:** June 1996; modified edits related to tuition classification, July 2002.				
Gender	**Definition:** The gender of the individual. **Codes/Notes:** 1 - Male 2 - Female Formerly identified as sex. Because IPEDS surveys do not provide an unknown gender option, DHE-generated IPEDS facsimiles are based on the following procedure, implemented March 2002 with the Fall 2001Enrollment File and FY2002 Degree File uploaded to NCES. Students whose ID ends with an even digit will be reported to NCES as male; students with an ID that ends with an odd number will be reported as female. **Missing Value:** Blank, if unknown. **Edit Specs:** Error if not blank or not = '1' or '2'. **Updates:** October 31, 1985; modified IPEDS proration methodology, March 2002.	Numeric	1		N
Citizenship Status	**Definition:** Citizenship is the status of being a citizen, along with the rights, duties and privileges of being a citizen.	Numeric	1	N	N

	Codes/Notes: 1 - Nationality 2- Naturalization 3- Dual 4- Immigration 5 - Illegal immigration **Missing Value:** Does not apply; field must be completed. **Edit Specs:**				

Appendix K: HIPAA BA Interagency MOU

HIPAA BUSINESS ASSOCIATE
Interagency Memorandum of Understanding

The parties to this Business Associate Interagency Memorandum of Understanding ("MOU") are the Colorado Department of Human Services ("State," "Covered Entity" or "CE") and the Governor's Office of Information Technology ("Contractor," "or "Asssociate"). This MOU is effective as of August 6th, 2009 or the compliance date of the Privacy Rule (defined below), whichever first occurs (the "MOU Effective Date").

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 the Contract in compliance with the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320d – 3120d-8 ("HIPAA") and its implementing regulations thereunder by the U.S. Department of Health and Human Services (the "Privacy Rule") and other applicable laws, as amended.

C. As part of the HIPAA regulations, the Privacy Rule requires CE 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 MOU.

D. Authority exists in the Law and Funds have been budgeted, appropriated and otherwise made available and a sufficient uncommitted balance thereof remains available for encumbering and subsequent payment of this contract under Encumbrance Number ___N/A_____ in Fund Number _____N/A_____, Appropriation Account ___N/A_____ and Organization Number ___ N/A_____.

E. Required approval, clearance and coordination has been accomplished from and with appropriate agencies.

The parties agree as follows:

1. Definitions.

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

2. Statement of Work and Responsibilities. [Detailed statement of work]

3. Payment Amount and Billing Procedure. [In consideration of Associate performing its obligations under Section 2 above, CE will transfer $ 0.00 upon satisfactory completion of performance.]

4. Term. The term of this MOU begins on the MOU Effective Date, as set forth in the opening paragraph of this MOU, and runs through termination of MOU by the Colorado Department of Human Services.

5. Obligations of Associate.

a. Permitted Uses. Associate shall not use Protected Information except for the purpose of performing Associate's obligations under and as permitted by the terms of this MOU. Further, Associate shall not use Protected Information in any manner that would constitute a violation of the Privacy Rule 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.

b. Permitted Disclosures. Associate shall not disclose Protected Information in any manner that would constitute a violation of the Privacy Rule if disclosed by CE, except that Associate may disclose Protected Information: (i) in a manner permitted pursuant to this MOU; (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, Associate must obtain, prior to making any such disclosure:(i) reasonable assurances from such third party that such Protected Information will be held confidential as provided pursuant to this MOU and only

disclosed as required by law or for the purposes for which it was disclosed to such third party; and (ii) an agreement from such third party to notify Associate within two 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 otherwise than as permitted by this MOU. 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.

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 MOU 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 this MOU, 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 MOU 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. Associate shall implement and maintain appropriate 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. Associate shall make Protected Information maintained by Associate or its agents or subcontractors in 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 Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.524.

g. Amendment of PHI. 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, Associate or its agents or subcontractors shall make such Protected Information available to CE for amendment and incorporate any such amendment to enable CE to fulfill its obligations with respect to requests by individuals to amend their PHI under the Privacy Rule, 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 the 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. Within ten (10) business days of notice by CE of a request for an accounting of disclosures of Protected Information, Associate and its agents or subcontractors shall make available to CE the information required to provide an accounting of

disclosures to enable CE to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. Section 164.528. As set forth in, and as limited by, 45 C.F.R. Section 164.528, Associate shall not provide an accounting to CE of disclosures: (i) to carry out treatment, payment or health care operations, as set forth in 45 C.F.R. Section 164.506; (ii) to individuals of Protected Information about them as set forth in 45 C.F.R. Section 164.502; (iii) pursuant to an authorization as provided in 45 C.F.R. Section 164.508; (iv) to persons involved in the individual's care or other notification purposes as set forth in 45 C.F.R. Section 164.510; (v) for national security or intelligence purposes as set forth in 45 C.F.R. Section 164.512(k)(2); (vi) to correctional institutions or law enforcement officials as set forth in 45 C.F.R. Section 164.512(k)(5); (vii) incident to a use or disclosure otherwise permitted by the Privacy Rule; (viii) as part of a limited data set under 45 C.F.R. Section 164.514(e); or (ix) disclosures prior to April 14, 2003.. Associate agrees to implement a process that allows for an accounting to be collected and maintained by Associate and its agents or subcontractors for at least six (6) years prior to the request, but not before the compliance date of the Privacy Rule. At a minimum, such information shall include: (i) the date of disclosure; (ii) the name of the entity or person who received Protected Information and, if known, the address of the entity or person; (iii) a brief description of Protected Information disclosed; and (iv) a brief statement of purpose of the disclosure that reasonably informs the individual of the basis for the disclosure, or a copy of the individual's authorization, or a copy of the written request for disclosure. 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 5(b) of this MOU.

i. Governmental Access to Records. Associate shall 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 compliance with the Privacy Rule. 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.

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 Privacy Rule 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 as provided in Section 7(e) of this MOU, Associate and its subcontractors or agents shall retain all Protected Information throughout the term of this MOU and shall continue to maintain the information required under Section 5(h) of this MOU for a period of six (6) years after termination of the Contract.

m. Notification of Breach. During the term of this MOU, Associate shall notify CE within two business days of any suspected or actual breach of security, intrusion or unauthorized use or disclosure of PHI and/or any actual or suspected use or disclosure of data in violation of any applicable federal or state laws or regulations. 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.

n. Audits, Inspection and Enforcement. Within ten business (10) 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 MOU for the purpose of determining whether Associate has complied with this MOU; provided, however, that: (i) Associate and CE shall mutually agree in advance upon the scope, timing and location of such an inspection; (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; and (iii) CE shall execute a nondisclosure agreement, upon terms mutually agreed upon by the parties, if requested by Associate. 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 MOU, 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 this MOU.

o. Safeguards During Transmission. Associate shall be responsible for using appropriate safeguards to maintain and ensure the confidentiality, privacy and security of Protected Information transmitted to CE pursuant to this MOU, in accordance with the standards and requirements of the Privacy Rule, until such Protected Information is received by CE, and in accordance with any specifications set forth in Attachment A.

p. 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. 164.522, Associate will restrict the use or disclosure of an individual's Protected Information, provided Associate has agreed to such a restriction. 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.

6. Obligations of CE.

a. Safeguards During Transmission. CE shall be responsible for using appropriate safeguards to maintain and ensure the confidentiality, privacy and security of PHI transmitted to Associate pursuant to this MOU, in accordance with the standards and requirements of the

6. Additional Terms. *[This section may include specifications for disclosure format, method of transmission, use of an intermediary, use of digital signatures or PKI, authentication, additional security of privacy specifications, de-identification or re-identification of data and other additional terms.]*

The Colorado Department of Human Services (CDHS) Information Security Officer's (ISO) position is appropriated (funded) through the Health Insurance Portability and Accountability Act (HIPAA) long bill line item. As a HIPAA covered entity, CDHS must ensure compliance with the HIPAA rules and regulations. Fines and penalties are severe, ranging from $100 to $1,500,000 per violation.

It is imperative that the focus of the CDHS ISO remains specialized to ensure compliance to the HIPAA Privacy, Security and Enforcement Rules.

CDHS understands that there may be specifics projects that OIT would like the ISO to participate in. These projects shall align with the Departments HIPAA requirements.

Appendix L: Data Governance Road Map

- Defining Governance focus area
- Creating the Governance Team
    1. Start small
    2. Find a cross-section of stakeholders
    3. Find the personnel who really understand the data
    4. Understand where problem areas may be in the data by listening to stakeholders and stewards
    5. Vet all final decisions
- Integrating Data Stewardship into a Data Governance Program
- Creating the Governance and Stewardship Project Plan
- Constructing Appropriate Governance Documents
- Identifying Data sets and Meta Data Sources
- Planning the Maintenance of a Data Governance and Stewardship Program
- Future of Data Governance and Stewardship