Colorado Department of Health Care Policy and Financing

Solicitation #:

HCPFRFPKC13PBMS

Pharmacy Benefit Management System (PBMS)

Request for Proposals

Appendix G – PBMS Procurement Library Content List

SECTION G1.0 APPENDIX G – PROCUREMENT LIBRARY CONTENT LIST

G1.1. OVERVIEW

G1.1.1. This appendix provides additional resources to assist Contractors in responding to the Pharmacy Benefit Management System (PBMS) RFP.

Manual/Form Name	RFP Section Reference, If Applicable	Documentation Location (for this RFP)
1. Current MMIS and Fiscal Agent Contract Documents	N/A	http://www.colorado.gov/cs/Satellite/HCPF/HCPF/1251630478148
2. MMIS System Documentation and Operations Manual a. Specific PBMS System Documentation can be found in Chapters 12, 13, and 14	N/A	http://www.colorado.gov/cs/Satellite/HCPF/HCPF/1251630478148
3. Colorado Procurement Laws and Rules	N/A	http://www.colorado.gov/cs/Satellite/DPA-DFP/DFP/1251594746441
4. Medical Assistance program Client Caseload and Expenditure Reports as submitted monthly to the Joint Budget Committee	N/A	http://www.colorado.gov/cs/Satellite/HCPF/HCPF/1209635766663

5. Call Current Program Statistics with Center Data Reports	N/A	http://www.colorado.gov/cs/Satellite/HCPF/HCPF/1251630478148
6. Printing and Mailing Statistics	Pricing	Section G2.0 of Appendix G
7. Interfacing Systems Documentation	Section 4.4.3 – interfacing systems Section 4.6.6 – Interfacing Systems and Contracts	Section G3.0 of Appendix G
8. State Technology Standards and Requirements – Office of Information Security a. OIT Policy and Standards b. Information Security Policies c. System Security Plan Template	Appendix A – Requirements and Performance Standards; requirements 1023, 1034, 1194, 1196, and 1202	a. http://www.colorado.gov/cs/Satellite/OIT-Main/CBON/1251579386760 b. http://www.colorado.gov/cs/Satellite/OIT-Cyber/CBON/1251575408771 c. Section G4.0 of Appendix G
9. Operational Claims/Encounters Processing Volume Forecast (SFY 2014-15 through SFY 2020-21)	Section 10.6.5 and Pricing	Section G5.0 of Appendix G
10. ACA Provider Screening Rule State Plan, Department's general implementation plan, and Department's response to CMS' request for additional information	Section 5.2.7.1 – Online Provider Enrollment	Section G6.0 of Appendix G

11. Colorado Medical Assistance Program Provider Services and Web Portal	N/A	http://www.colorado.gov/cs/Satellite/HCPF/HCPF/1201542697178
12. Department Information a. Department Organizational Chart b. Department FTE Count by Office, Page B-3 c. Claims Systems and Operations Division Organization Chart d. General Department Information, 2011 Annual Report e. General Department Information, FY 2013-14 Budget Request f. Joint Budget Committee Staff Briefing Document, Description of Department FTE (page 31 and 32) and other information g. Department Budget Request for MMIS Reprocurement, R-5	Section 3.1.4 – Background Information Sections 3.5.1.1, and 3.5.1.2 – Project and State Resources Section 5.2.3 – Contract Stages	a. http://www.colorado.gov/cs/Satellite/HCPF/HCPF/1197364086669 b. http://www.colorado.gov/cs/Satellite?c=Document_C&childpagename=HCPF%2FDocument_C%2FHCPFAddLink&cid=1251633477624&pagename=HCPFWrapper c. Section G7.0 of Appendix G d. http://www.colorado.gov/cs/Satellite/HCPF/HCPF/1197364086669 e. http://www.colorado.gov/cs/Satellite/HCPF/HCPF/1251633122652 f. http://www.tornado.state.co.us/gov_dir/leg_dir/jbc/2012-13/hcpbrf.htm g. http://www.colorado.gov/cs/Satellite/HCPF/HCPF/1251633549972

13. Miscellaneous Documents, MMIS Procurement Analysis Report, MITA State Self-Assessment	N/A	http://www.colorado.gov/cs/Satellite/HCPF/HCPF/1251627905874
14. Office of Information Technology – Gate Review Slides		h. Section G8.0 of Appendix G
15. MMIS Turnover Plan		i. Section G9.0 of Appendix G

Section G2.0

	Total Pages	Total Packages	Additional Pages	Total Postage Used
Dec-12	73,006	50,538	22,468	$18,652
Nov-12	98,381	68,849	29,532	$25,391
Oct-12	90,054	63,547	26,507	$23,408
Sep-12	75,663	50,398	25,265	$18,534
Aug-12	69,817	46,432	23,385	$16,779
Jul-12	85,373	57,629	27,744	$21,145
Total July - December 2012	**492,294**	**337,393**	**154,901**	**$123,910**

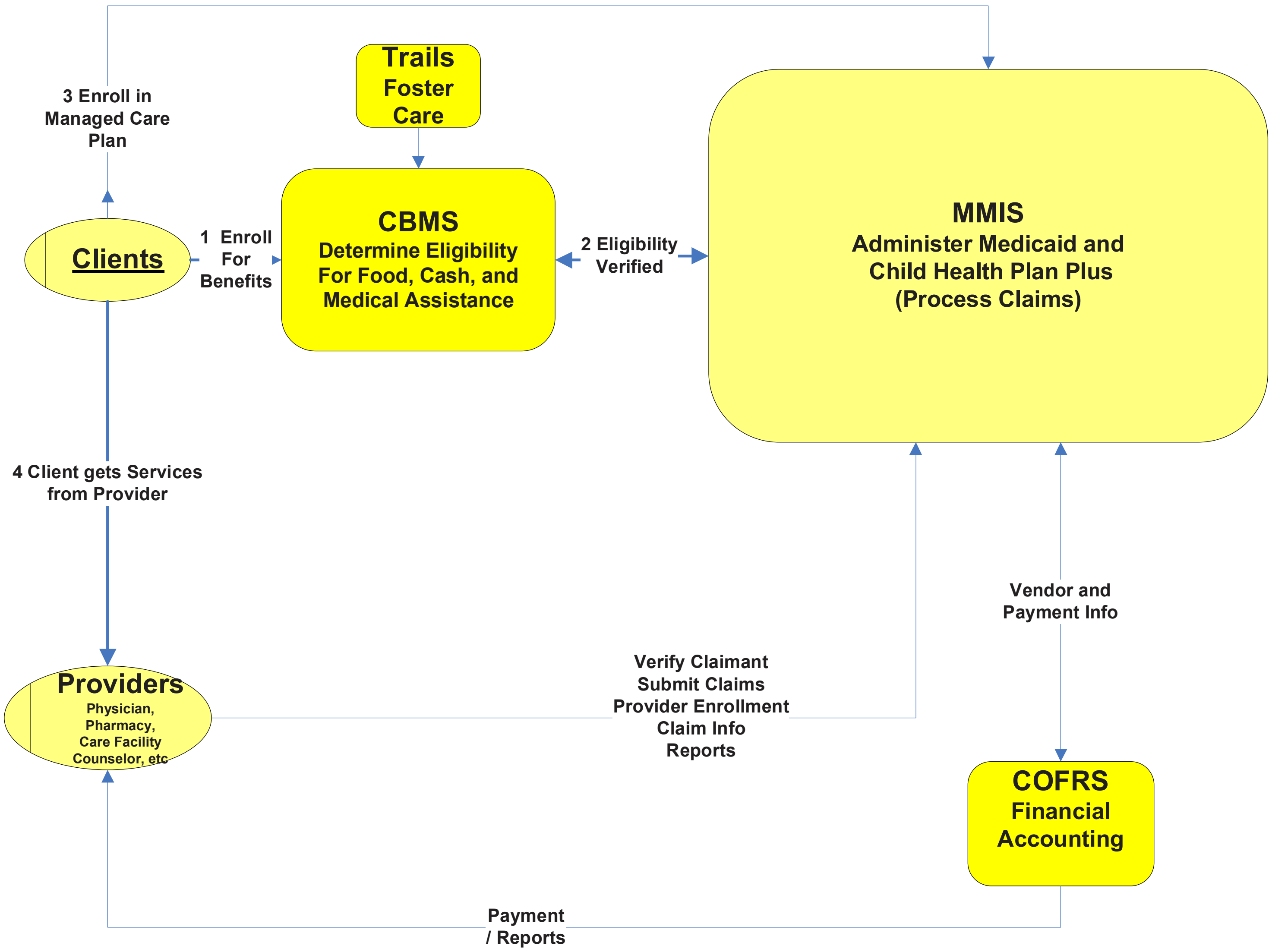
Printing / Postage (July 2012 - December 2012)

Printed Pages	647,195
Mailed Envelopes/Packages	337,393
Postage Cost	$123,910

MMIS Overview

MMIS - THE VERY BASICS

(Highest Level)



Trails Foster Care

CBMS
Determine Eligibility For Food, Cash, and Medical Assistance

MMIS
Administer Medicaid and Child Health Plan Plus (Process Claims)

Clients

1 Enroll For Benefits

2 Eligibility Verified

3 Enroll in Managed Care Plan

4 Client gets Services from Provider

Providers
Physician, Pharmacy, Care Facility Counselor, etc

Verify Claimant
Submit Claims
Provider Enrollment
Claim Info
Reports

Vendor and Payment Info

COFRS
Financial Accounting

Payment / Reports

Boards and Committees (18X) HCPF External Website

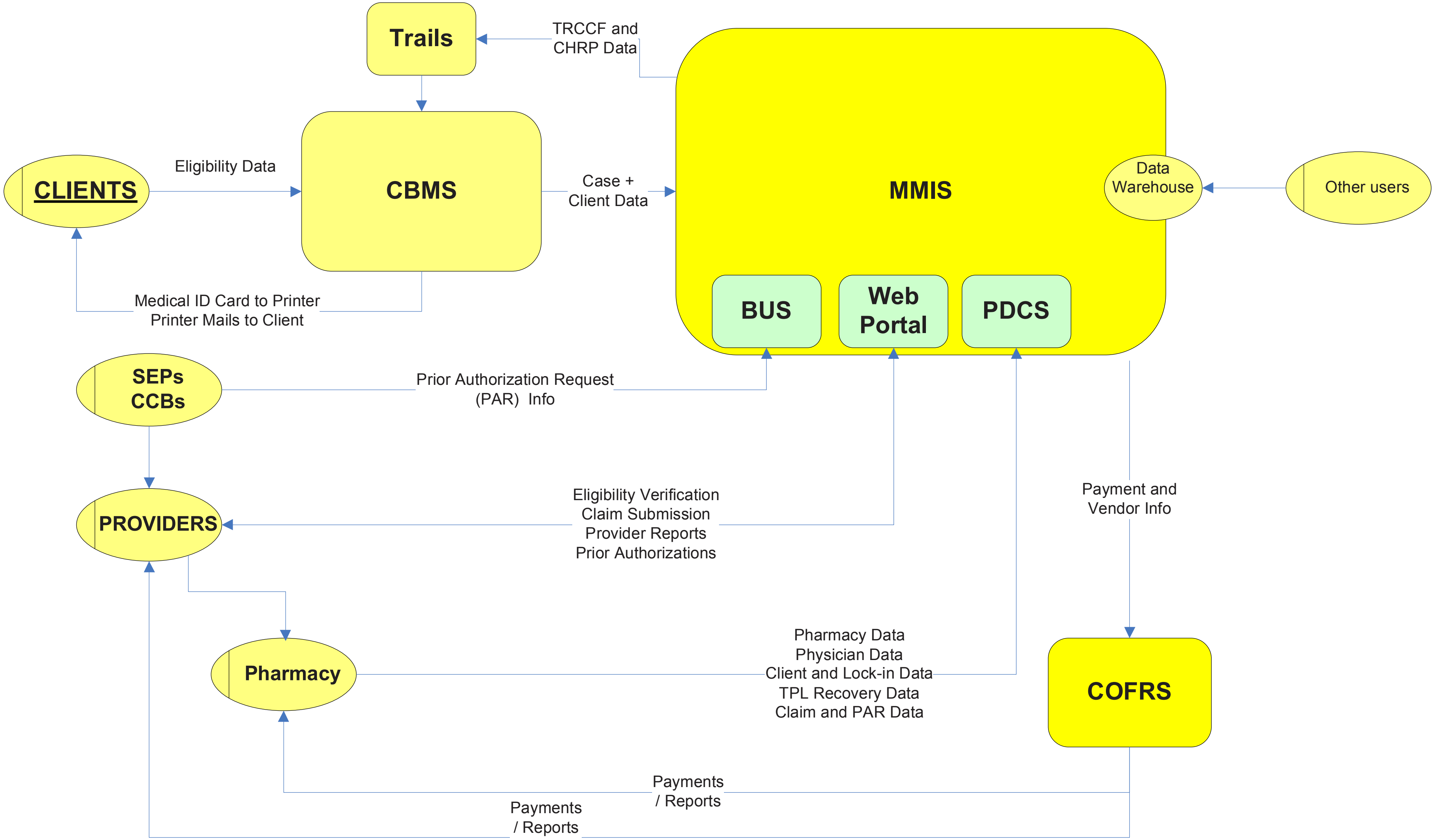
Partners and Researchers(~7x) HCPF External Website

Federal Gov SSA / CMS

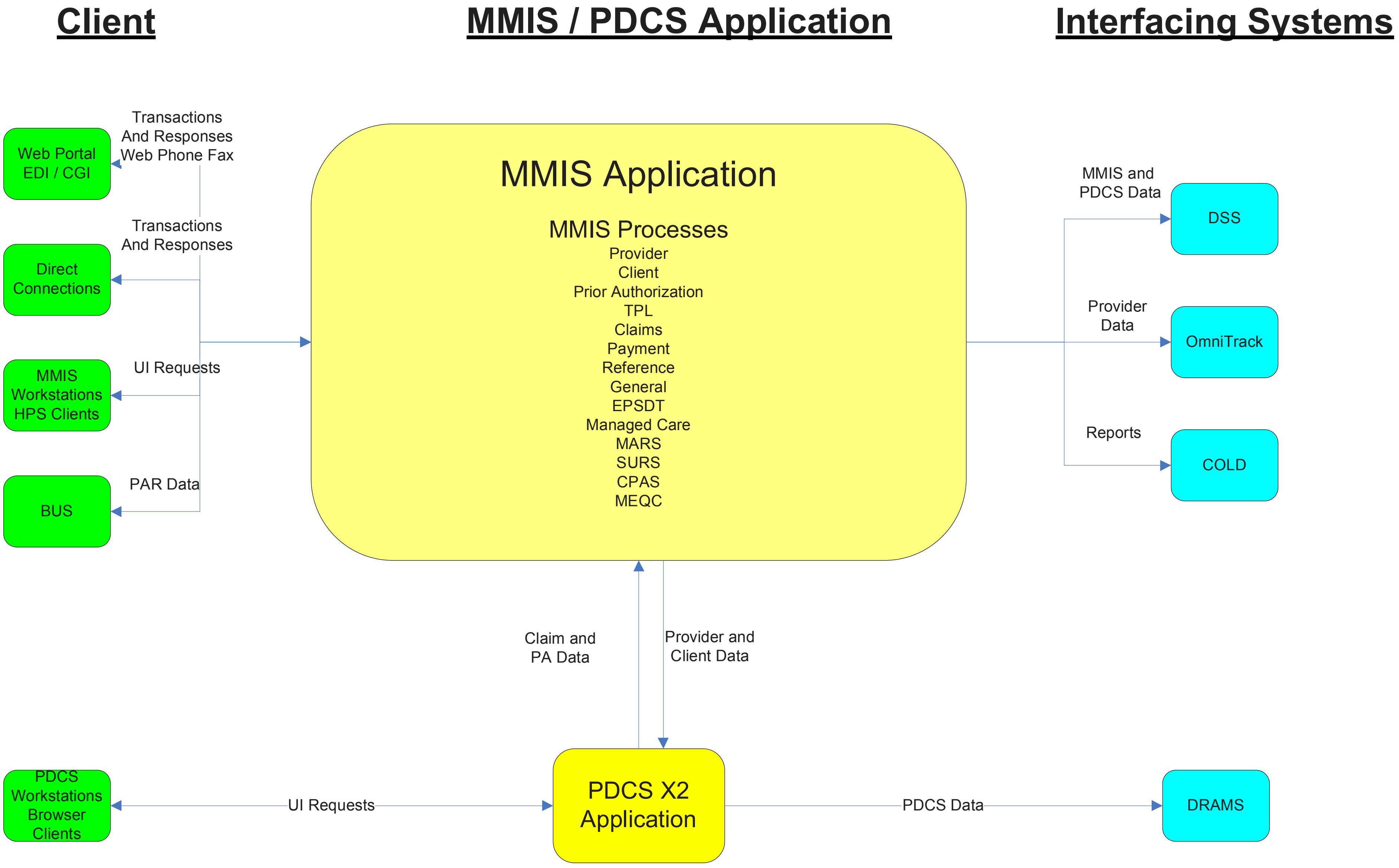
State Auditior

MMIS Overview

MMIS - A LITTLE MORE DETAIL



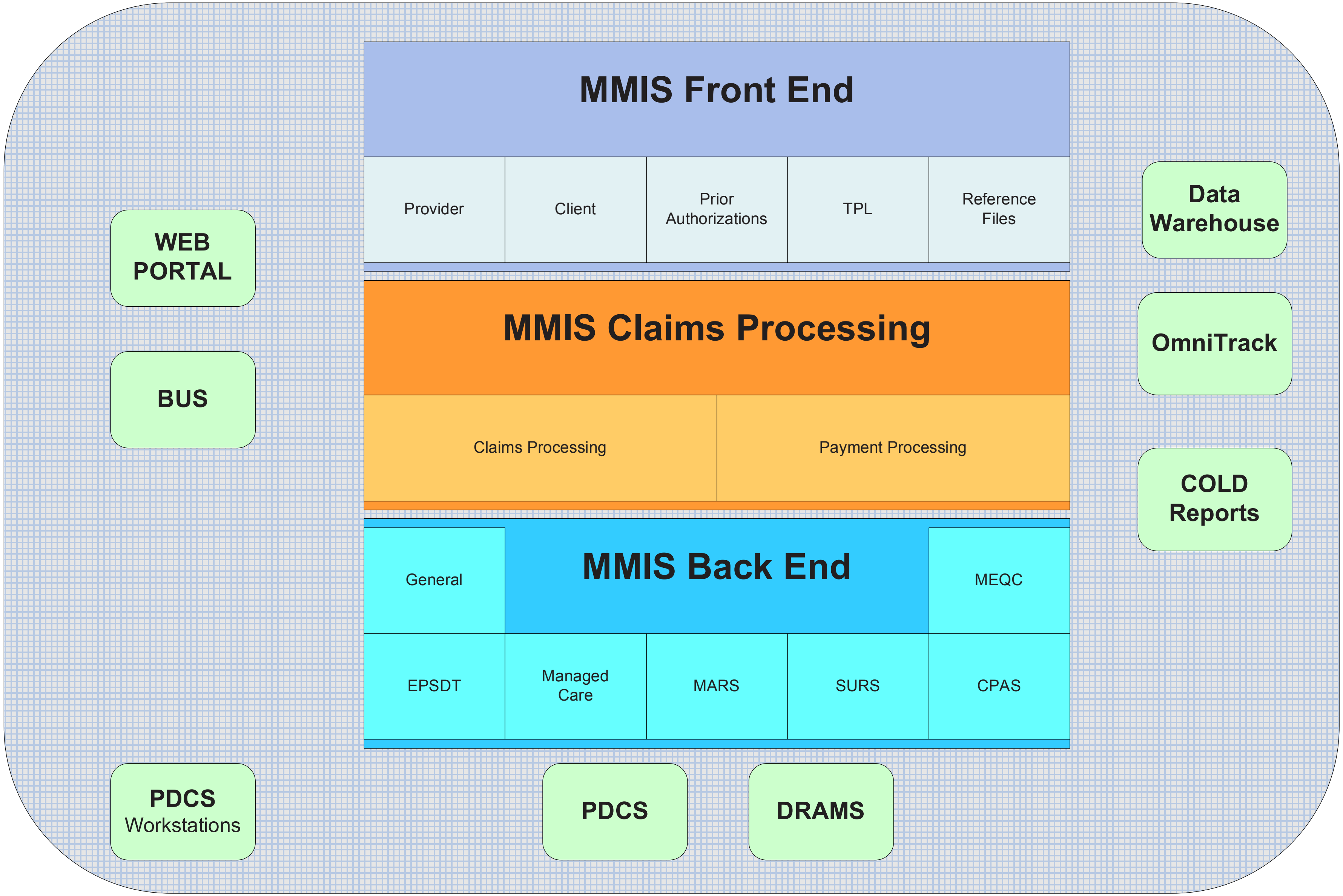
MMIS Overview



The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

MMIS Overview

MAJOR COMPONENTS of MMIS



MMIS Front End

Provider

Client

Prior Authorizations

TPL

Reference Files

MMIS Claims Processing

Claims Processing

Payment Processing

MMIS Back End

General

MEQC

EPSDT

Managed Care

MARS

SURS

CPAS

WEB PORTAL

BUS

PDCS Workstations

PDCS

DRAMS

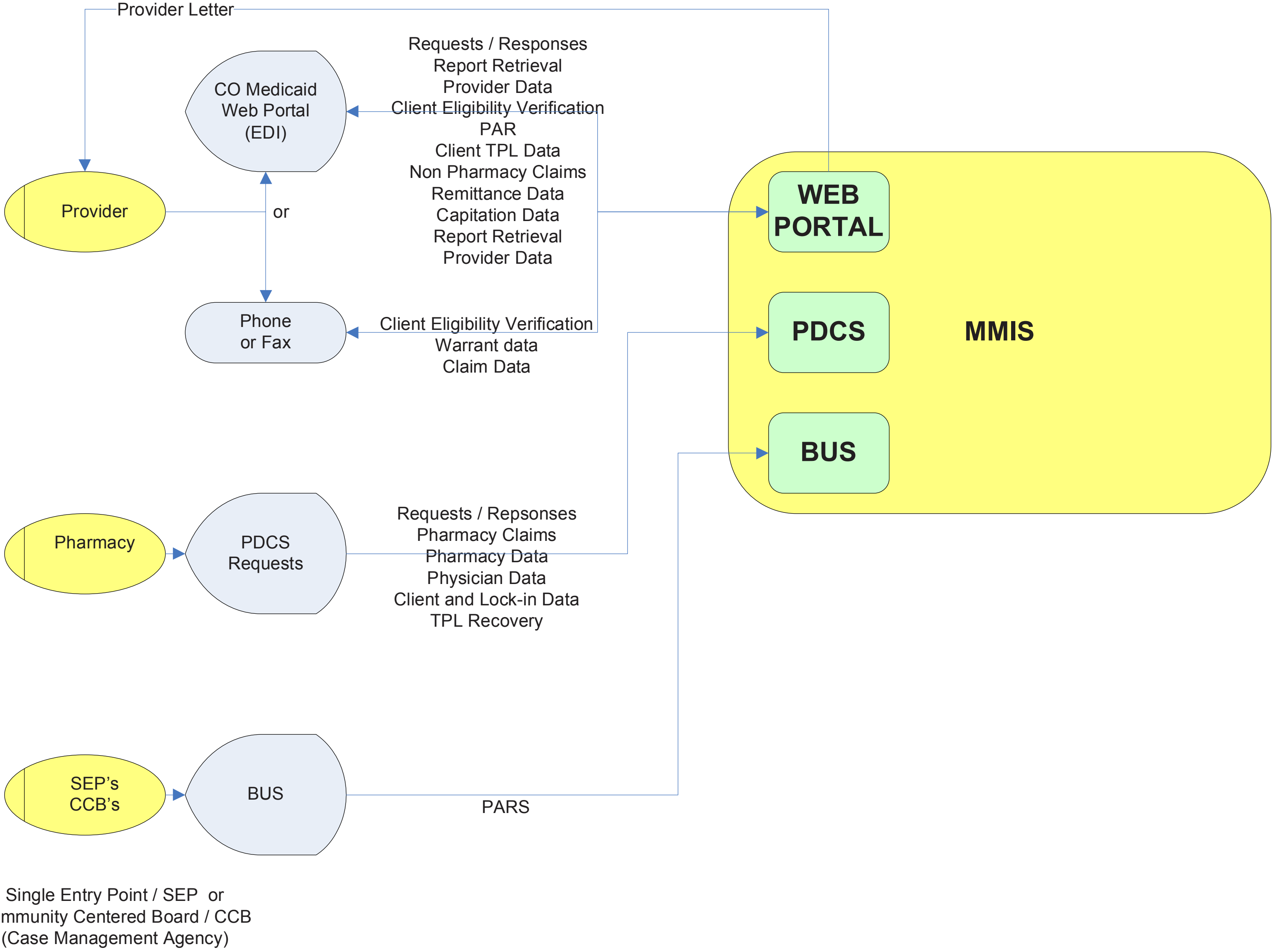
Data Warehouse

OmniTrack

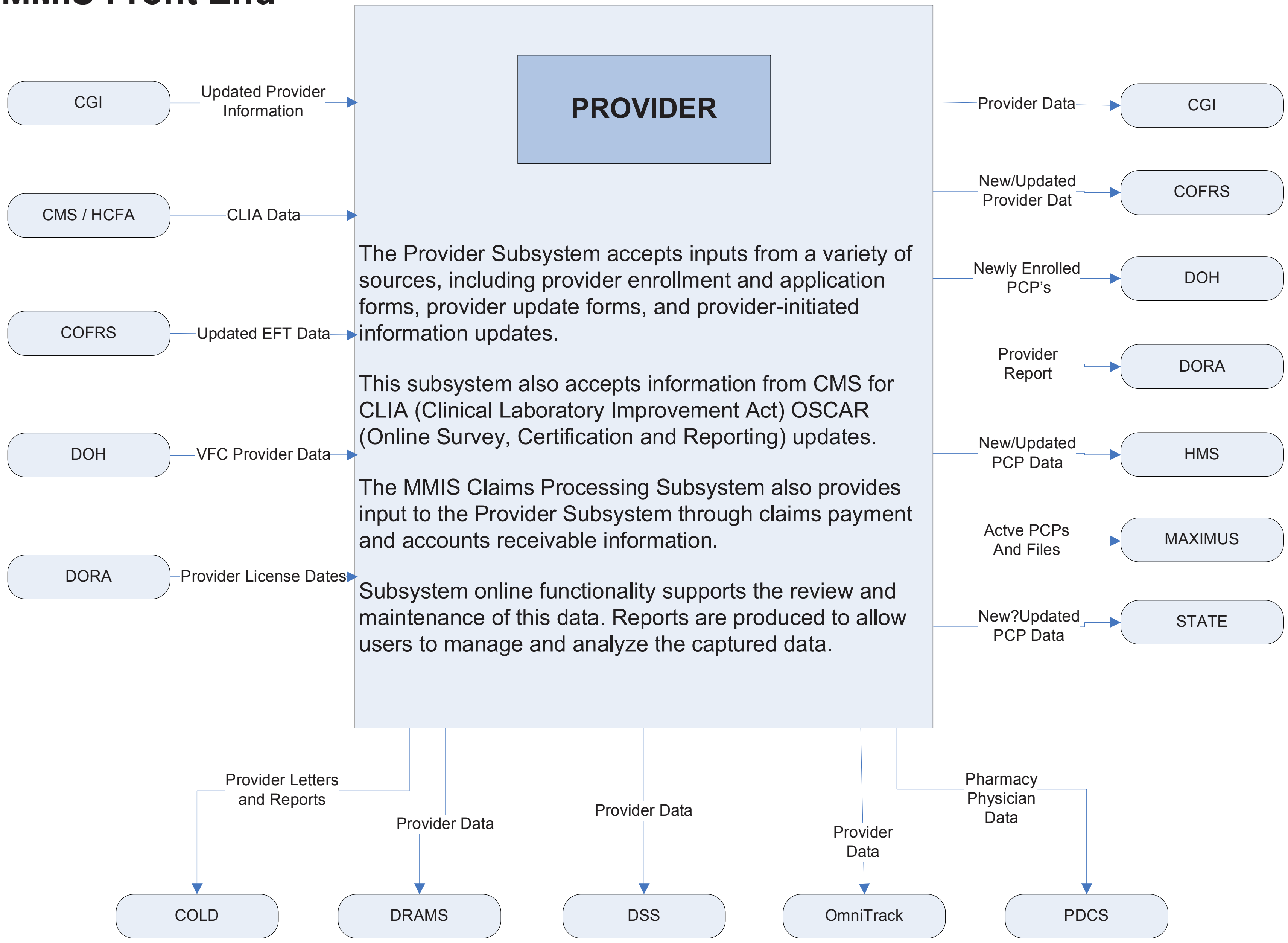
COLD Reports

MMIS Front End

MMIS Web Access



MMIS Front End



The Provider Subsystem accepts inputs from a variety of sources, including provider enrollment and application forms, provider update forms, and provider-initiated information updates.

This subsystem also accepts information from CMS for CLIA (Clinical Laboratory Improvement Act) OSCAR (Online Survey, Certification and Reporting) updates.

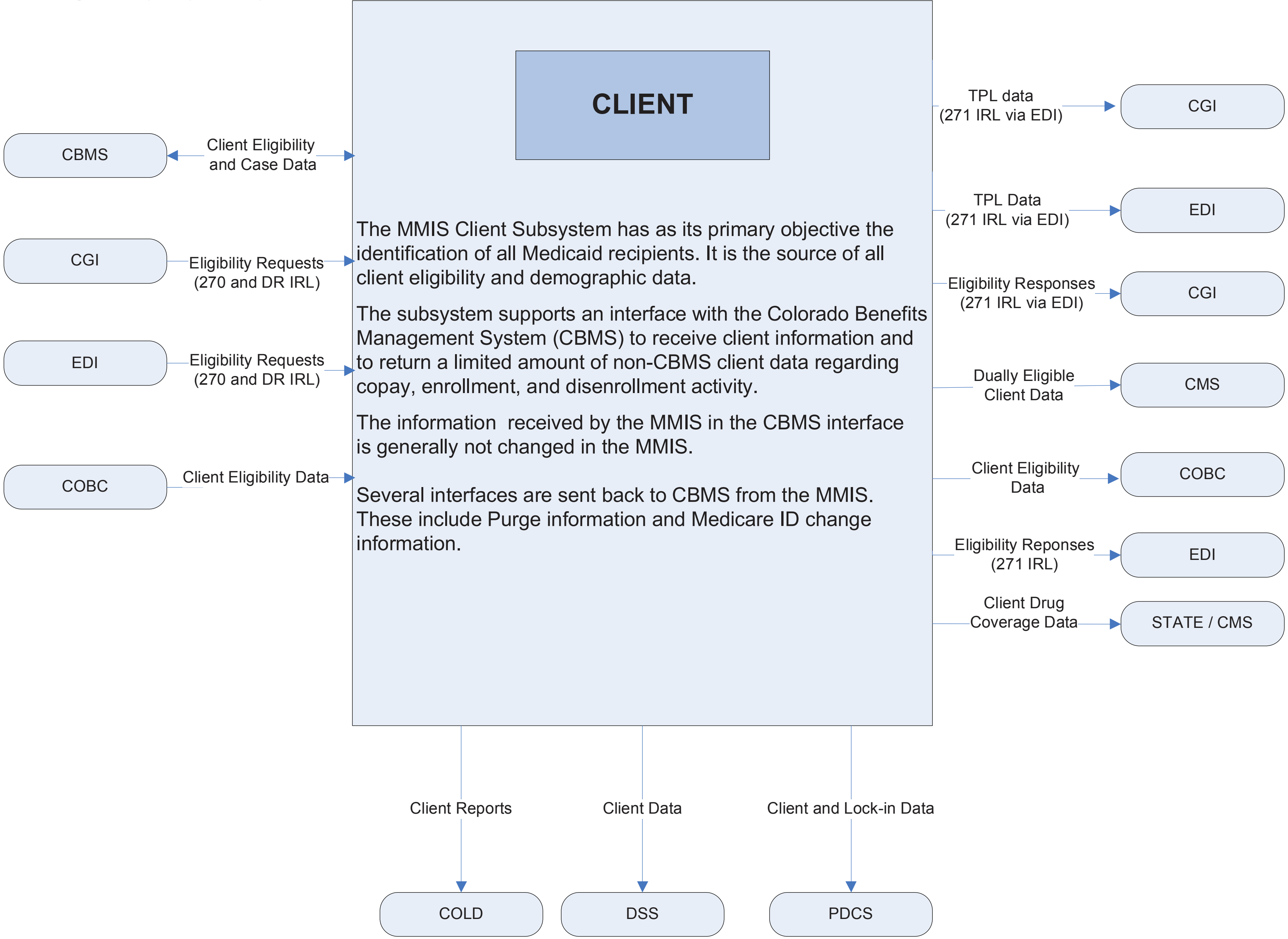
The MMIS Claims Processing Subsystem also provides input to the Provider Subsystem through claims payment and accounts receivable information.

Subsystem online functionality supports the review and maintenance of this data. Reports are produced to allow users to manage and analyze the captured data.

From ACS Medicaid
Processing Overview
11/07/2008 pg 11

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

MMIS Front End



CLIENT

The MMIS Client Subsystem has as its primary objective the identification of all Medicaid recipients. It is the source of all client eligibility and demographic data.

The subsystem supports an interface with the Colorado Benefits Management System (CBMS) to receive client information and to return a limited amount of non-CBMS client data regarding copay, enrollment, and disenrollment activity.

The information received by the MMIS in the CBMS interface is generally not changed in the MMIS.

Several interfaces are sent back to CBMS from the MMIS. These include Purge information and Medicare ID change information.

CBMS — Client Eligibility and Case Data

CGI — Eligibility Requests (270 and DR IRL)

EDI — Eligibility Requests (270 and DR IRL)

COBC — Client Eligibility Data

TPL data (271 IRL via EDI) — CGI

TPL Data (271 IRL via EDI) — EDI

Eligibility Responses (271 IRL via EDI) — CGI

Dually Eligible Client Data — CMS

Client Eligibility Data — COBC

Eligibility Reponses (271 IRL) — EDI

Client Drug Coverage Data — STATE / CMS

Client Reports — COLD

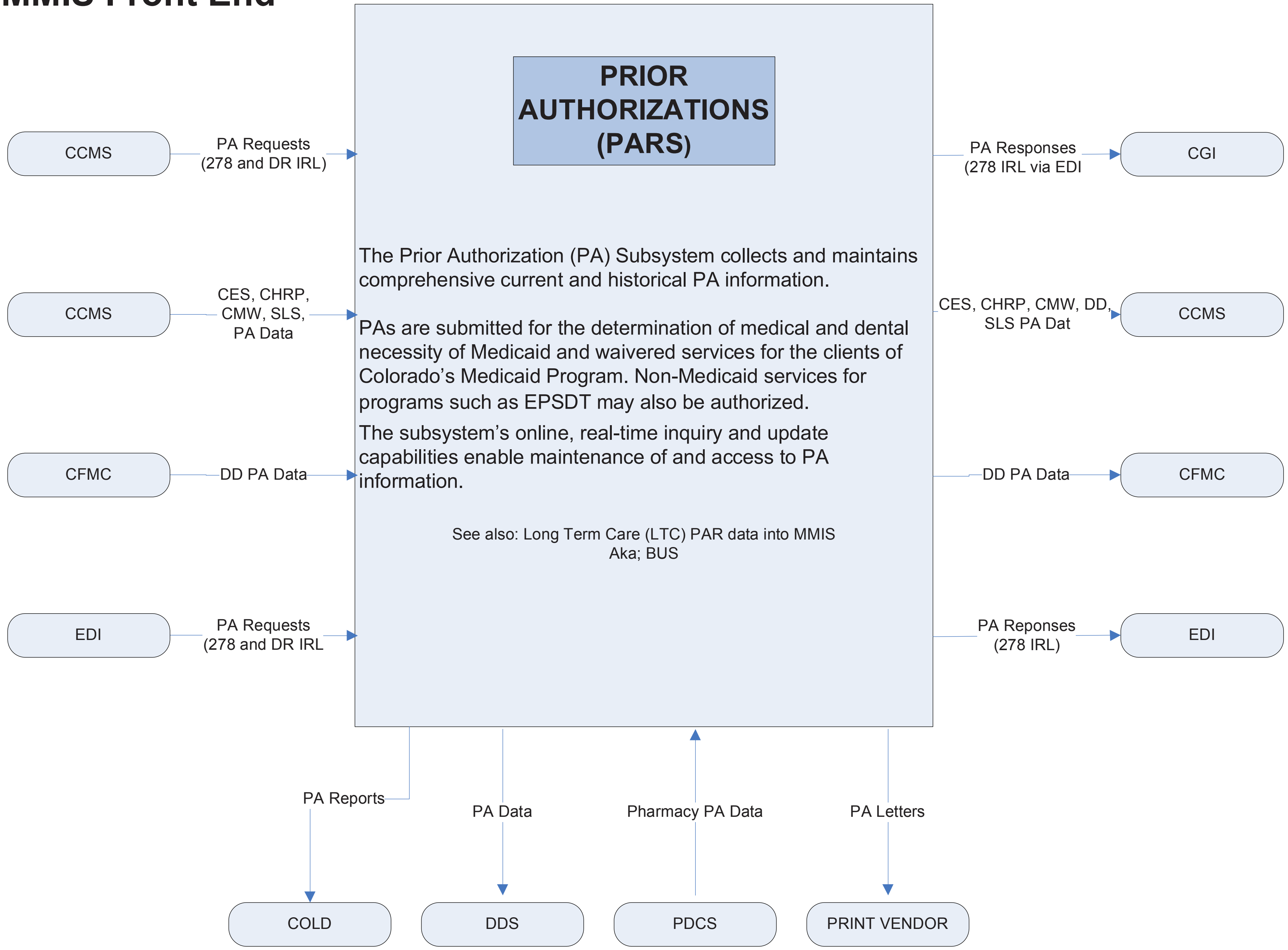
Client Data — DSS

Client and Lock-in Data — PDCS

From ACS Medicaid
Processing Overview
11/07/2008 pg 12

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

MMIS Front End



PRIOR AUTHORIZATIONS (PARS)
CCMS
PA Requests (278 and DR IRL)
CCMS
CES, CHRP, CMW, SLS, PA Data
CFMC
DD PA Data
EDI
PA Requests (278 and DR IRL
PA Responses (278 IRL via EDI
CGI
CES, CHRP, CMW, DD, SLS PA Dat
CCMS
DD PA Data
CFMC
PA Reponses (278 IRL)
EDI
PA Reports
PA Data
Pharmacy PA Data
PA Letters
COLD
DDS
PDCS
PRINT VENDOR

The Prior Authorization (PA) Subsystem collects and maintains comprehensive current and historical PA information.

PAs are submitted for the determination of medical and dental necessity of Medicaid and waivered services for the clients of Colorado's Medicaid Program. Non-Medicaid services for programs such as EPSDT may also be authorized.

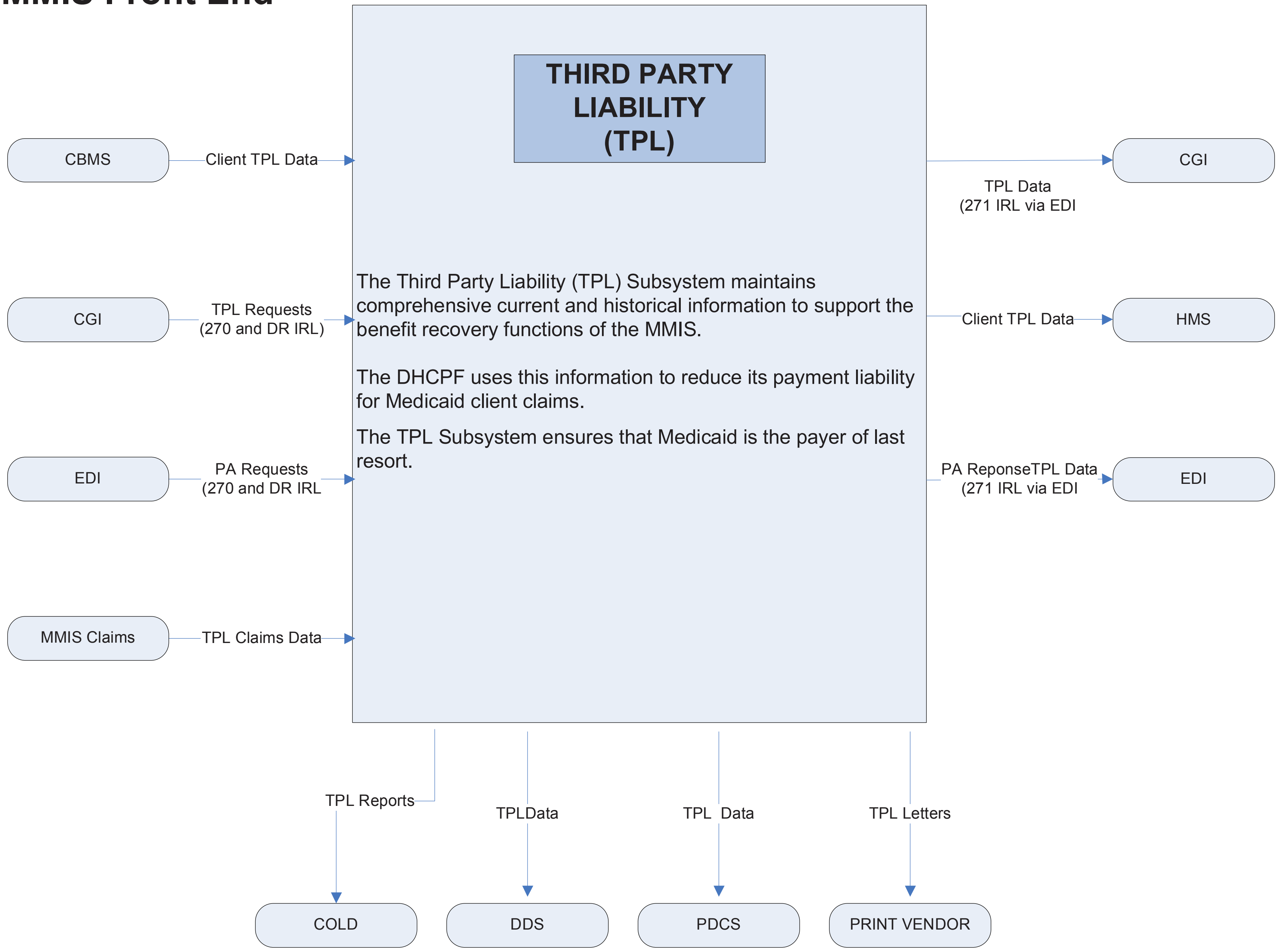
The subsystem's online, real-time inquiry and update capabilities enable maintenance of and access to PA information.

See also: Long Term Care (LTC) PAR data into MMIS
Aka; BUS

From ACS Medicaid
Processing Overview
11/07/2008 pg 13

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

MMIS Front End


THIRD PARTY LIABILITY (TPL)
CBMS
Client TPL Data
CGI
TPL Requests (270 and DR IRL)
EDI
PA Requests (270 and DR IRL
MMIS Claims
TPL Claims Data
CGI
TPL Data (271 IRL via EDI
HMS
Client TPL Data
EDI
PA ReponseTPL Data (271 IRL via EDI
TPL Reports
COLD
TPLData
DDS
TPL Data
PDCS
TPL Letters
PRINT VENDOR

The Third Party Liability (TPL) Subsystem maintains comprehensive current and historical information to support the benefit recovery functions of the MMIS.

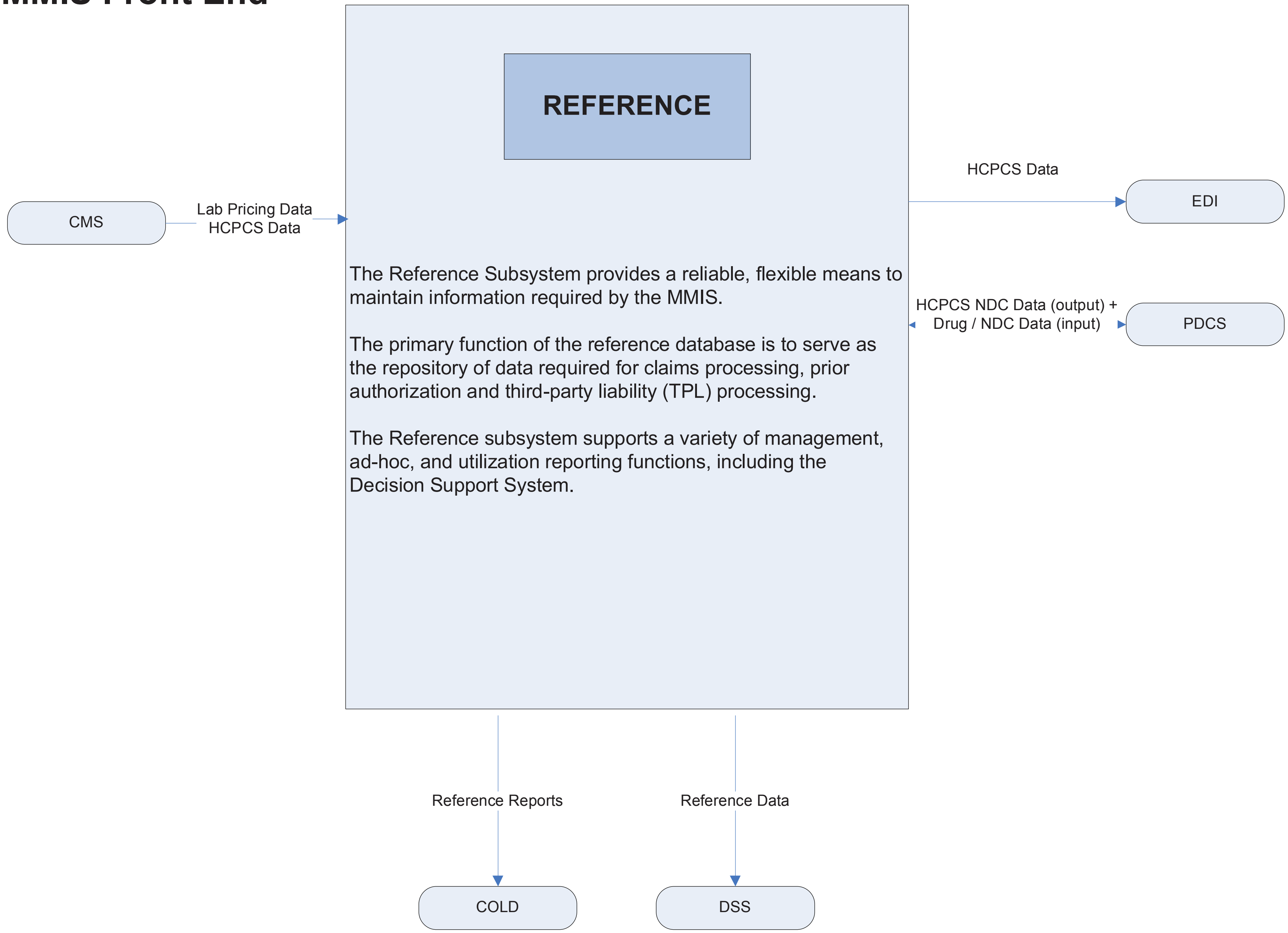
The DHCPF uses this information to reduce its payment liability for Medicaid client claims.

The TPL Subsystem ensures that Medicaid is the payer of last resort.

From ACS Medicaid Processing Overview 11/07/2008 pg 14

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

MMIS Front End



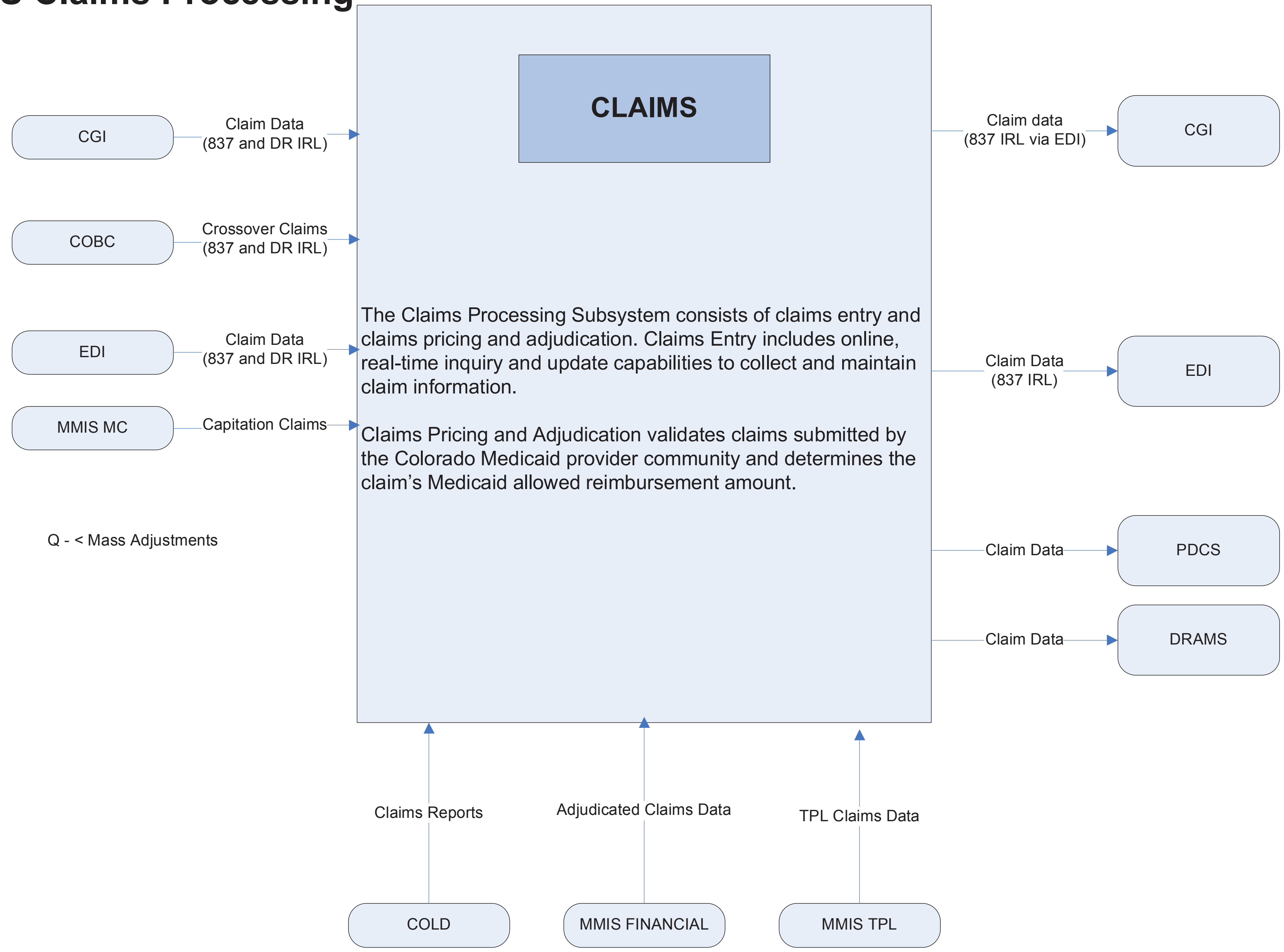
The Reference Subsystem provides a reliable, flexible means to maintain information required by the MMIS.

The primary function of the reference database is to serve as the repository of data required for claims processing, prior authorization and third-party liability (TPL) processing.

The Reference subsystem supports a variety of management, ad-hoc, and utilization reporting functions, including the Decision Support System.

From ACS Medicaid
Processing Overview
11/07/2008 pg 15

MMIS Claims Processing



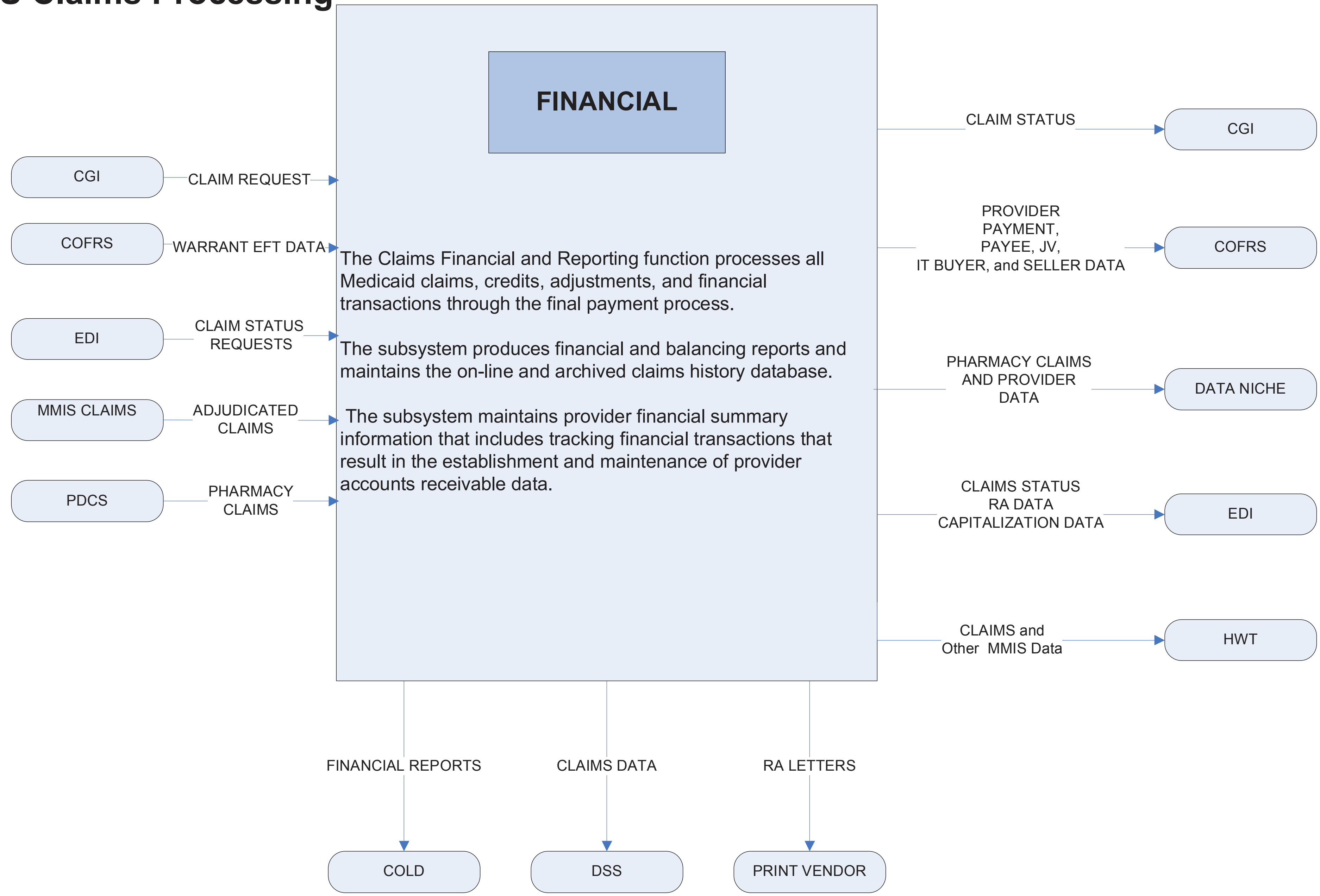
The Claims Processing Subsystem consists of claims entry and claims pricing and adjudication. Claims Entry includes online, real-time inquiry and update capabilities to collect and maintain claim information.

Claims Pricing and Adjudication validates claims submitted by the Colorado Medicaid provider community and determines the claim’s Medicaid allowed reimbursement amount.

From ACS Medicaid
Processing Overview
11/07/2008 pg 16

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

MMIS Claims Processing



FINANCIAL

CGI — CLAIM REQUEST →

COFRS — WARRANT EFT DATA →

EDI — CLAIM STATUS REQUESTS →

MMIS CLAIMS — ADJUDICATED CLAIMS →

PDCS — PHARMACY CLAIMS →

The Claims Financial and Reporting function processes all Medicaid claims, credits, adjustments, and financial transactions through the final payment process.

The subsystem produces financial and balancing reports and maintains the on-line and archived claims history database.

The subsystem maintains provider financial summary information that includes tracking financial transactions that result in the establishment and maintenance of provider accounts receivable data.

CLAIM STATUS → CGI

PROVIDER PAYMENT, PAYEE, JV, IT BUYER, and SELLER DATA → COFRS

PHARMACY CLAIMS AND PROVIDER DATA → DATA NICHE

CLAIMS STATUS RA DATA CAPITALIZATION DATA → EDI

CLAIMS and Other MMIS Data → HWT

FINANCIAL REPORTS → COLD

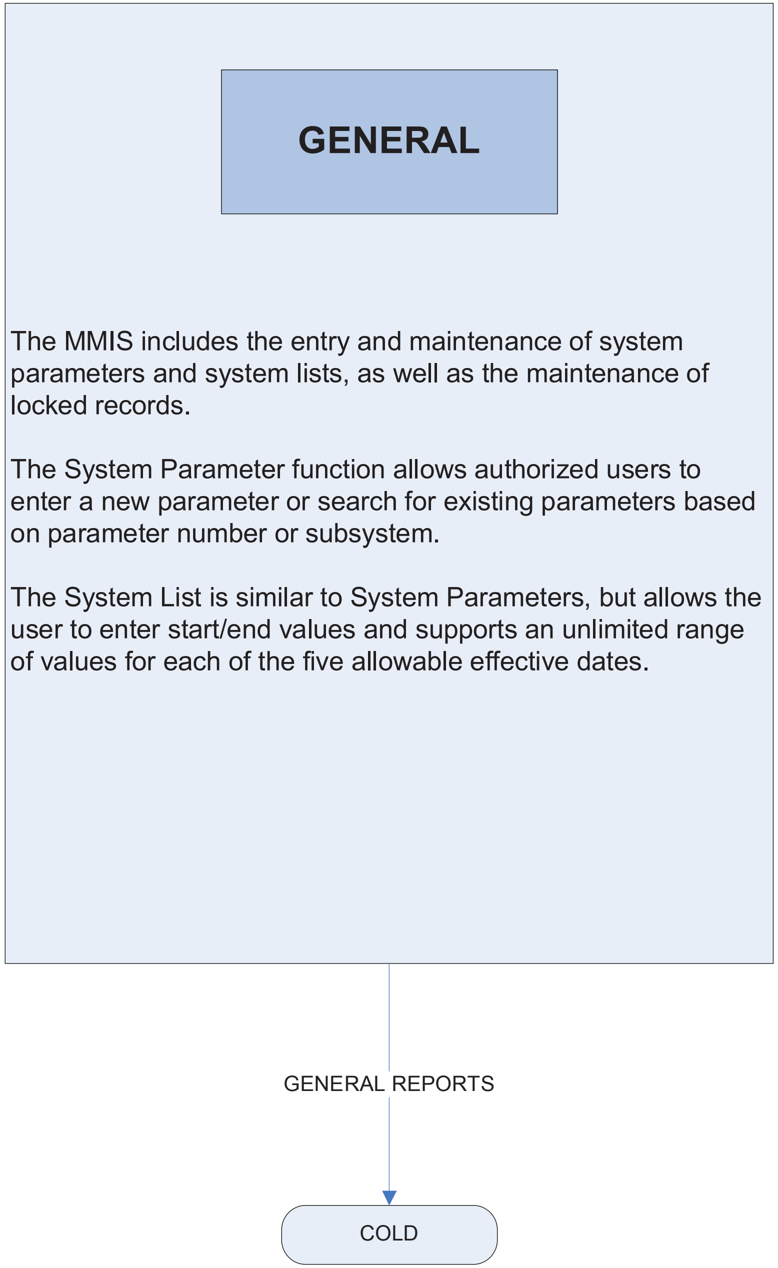
CLAIMS DATA → DSS

RA LETTERS → PRINT VENDOR

From ACS Medicaid Processing Overview 11/07/2008 pg 17

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

MMIS Back End



GENERAL

The MMIS includes the entry and maintenance of system parameters and system lists, as well as the maintenance of locked records.

The System Parameter function allows authorized users to enter a new parameter or search for existing parameters based on parameter number or subsystem.

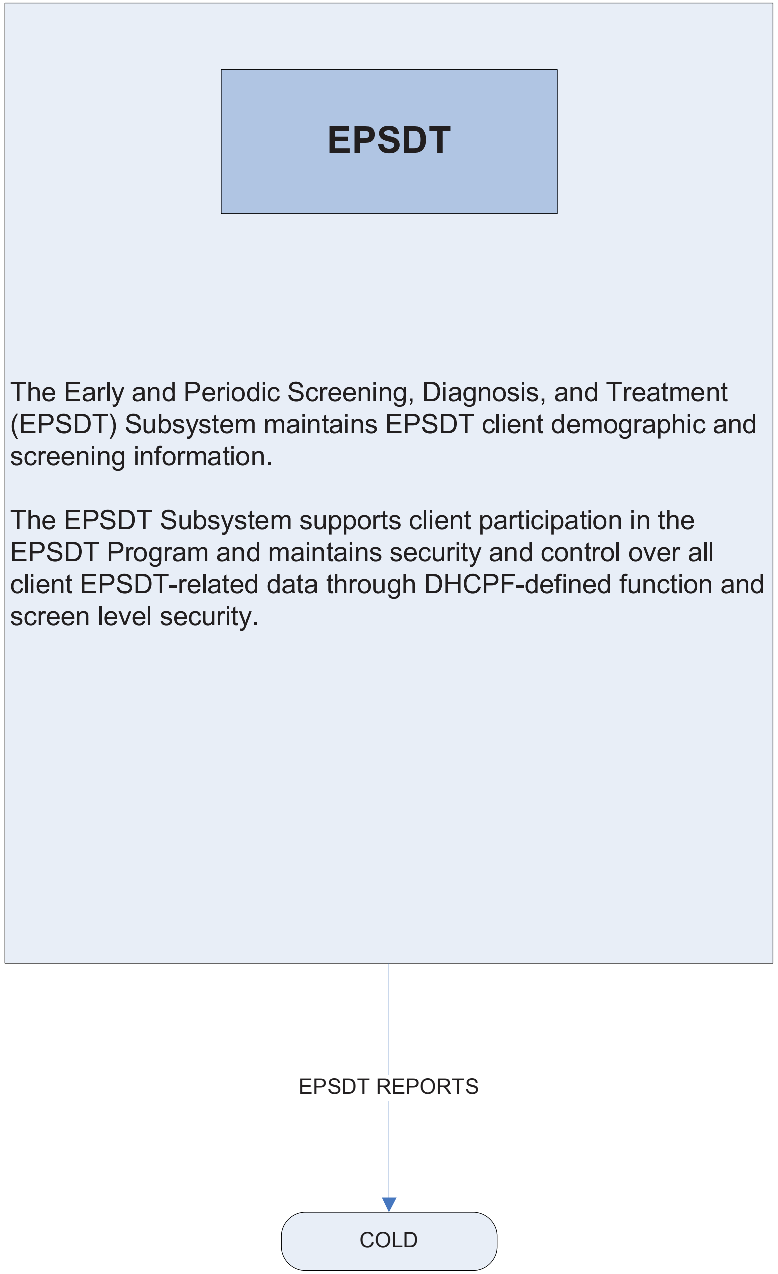
The System List is similar to System Parameters, but allows the user to enter start/end values and supports an unlimited range of values for each of the five allowable effective dates.

GENERAL REPORTS

COLD

From ACS Medicaid
Processing Overview
11/07/2008 pg 18

MMIS Back End



EPSDT

The Early and Periodic Screening, Diagnosis, and Treatment (EPSDT) Subsystem maintains EPSDT client demographic and screening information.

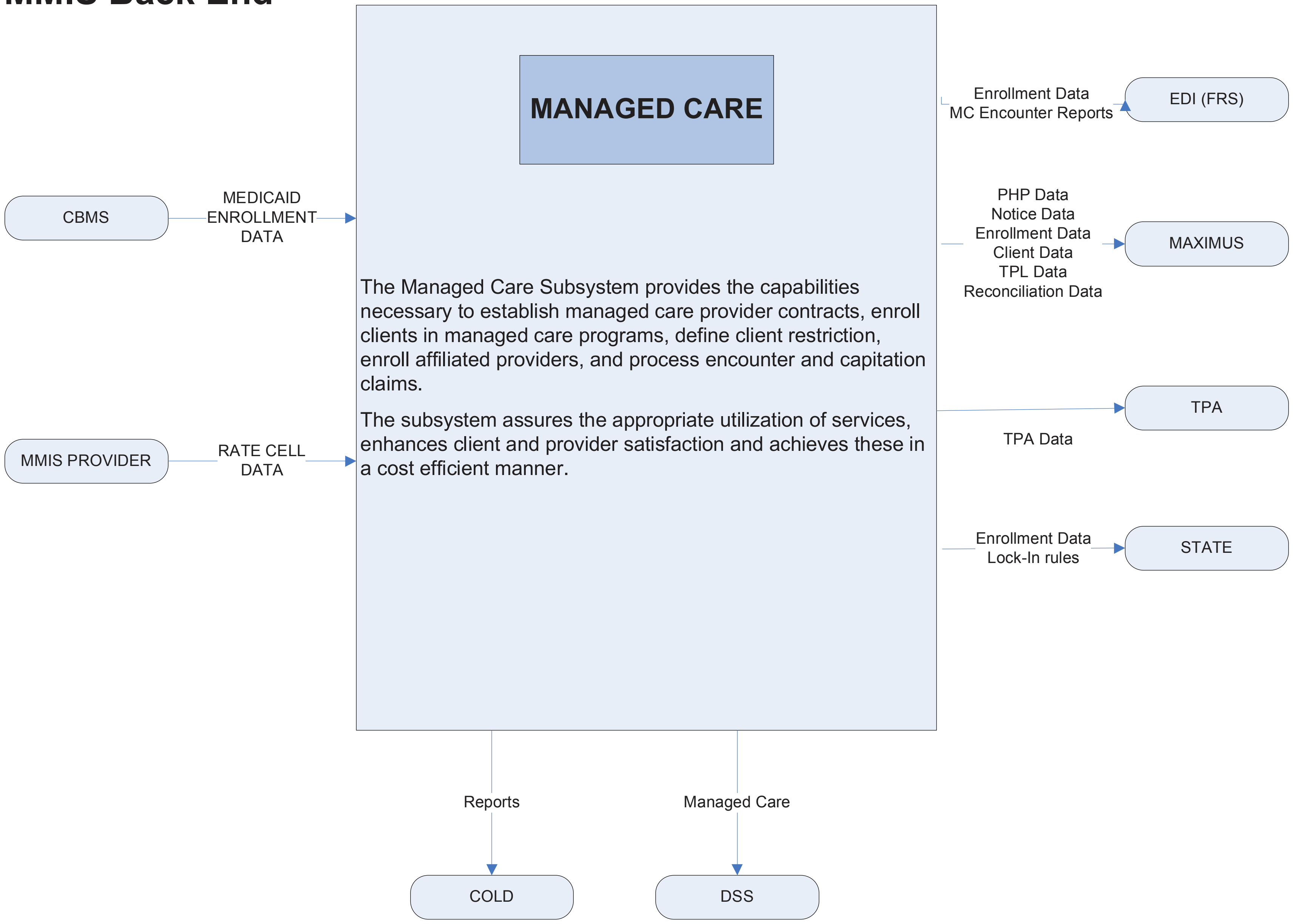
The EPSDT Subsystem supports client participation in the EPSDT Program and maintains security and control over all client EPSDT-related data through DHCPF-defined function and screen level security.

EPSDT REPORTS

COLD

From ACS Medicaid
Processing Overview
11/07/2008 pg 18

MMIS Back End



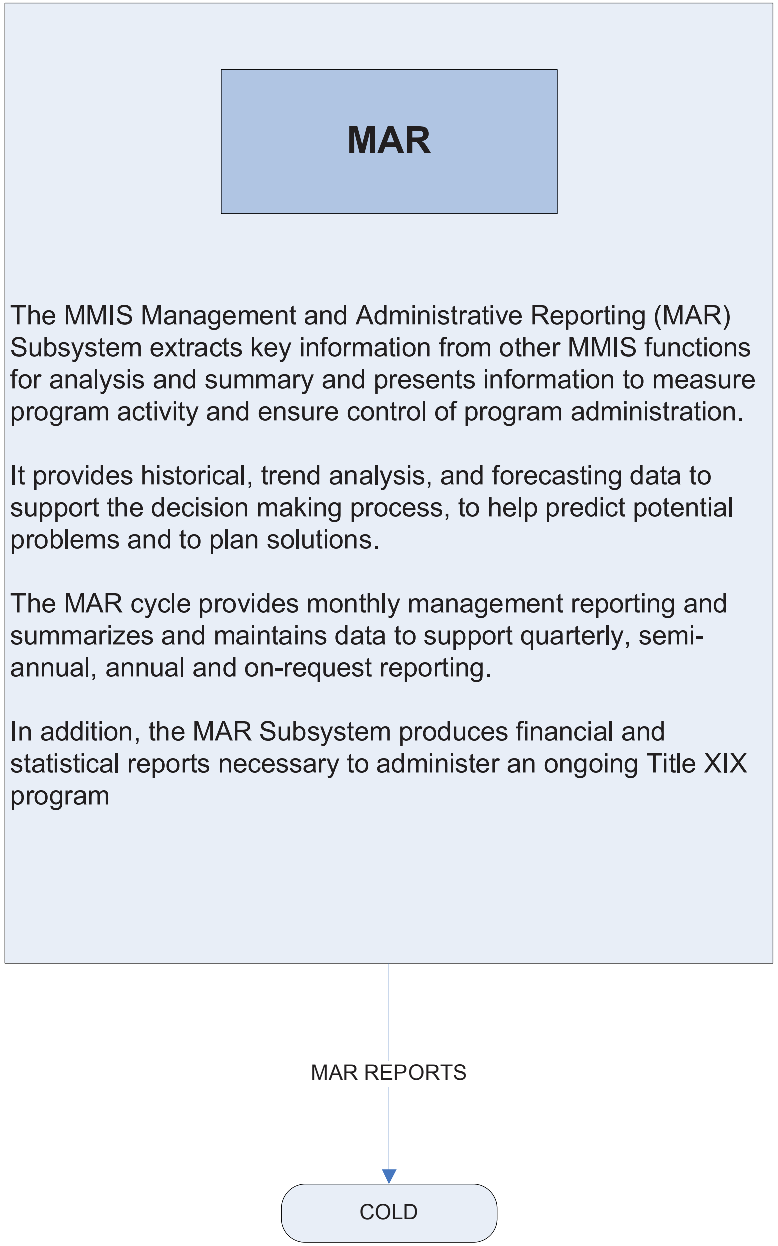
The Managed Care Subsystem provides the capabilities necessary to establish managed care provider contracts, enroll clients in managed care programs, define client restriction, enroll affiliated providers, and process encounter and capitation claims.

The subsystem assures the appropriate utilization of services, enhances client and provider satisfaction and achieves these in a cost efficient manner.

From ACS Medicial
Processing Overview

11/07/2008 pg 20

MMIS Back End



The MMIS Management and Administrative Reporting (MAR) Subsystem extracts key information from other MMIS functions for analysis and summary and presents information to measure program activity and ensure control of program administration.

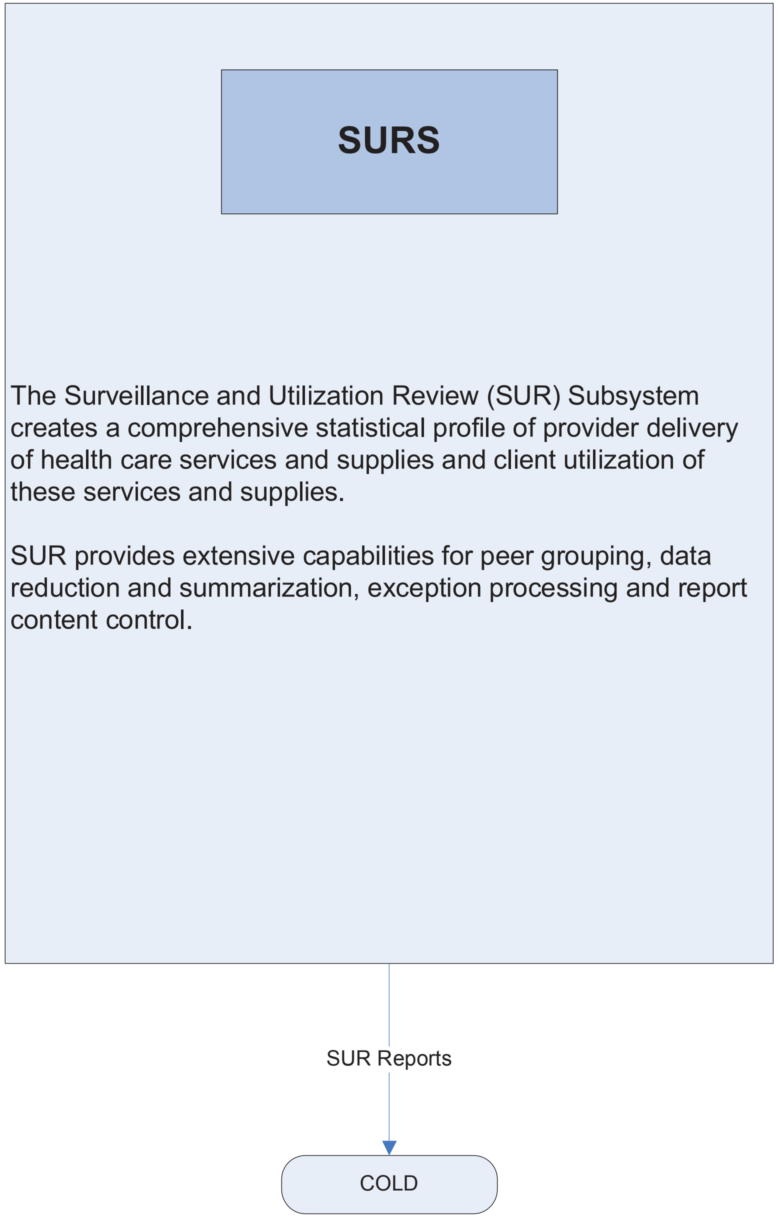
It provides historical, trend analysis, and forecasting data to support the decision making process, to help predict potential problems and to plan solutions.

The MAR cycle provides monthly management reporting and summarizes and maintains data to support quarterly, semi-annual, annual and on-request reporting.

In addition, the MAR Subsystem produces financial and statistical reports necessary to administer an ongoing Title XIX program

From ACS Medicaid
Processing Overview
11/07/2008 pg 21

MMIS Back End



SURS

The Surveillance and Utilization Review (SUR) Subsystem creates a comprehensive statistical profile of provider delivery of health care services and supplies and client utilization of these services and supplies.

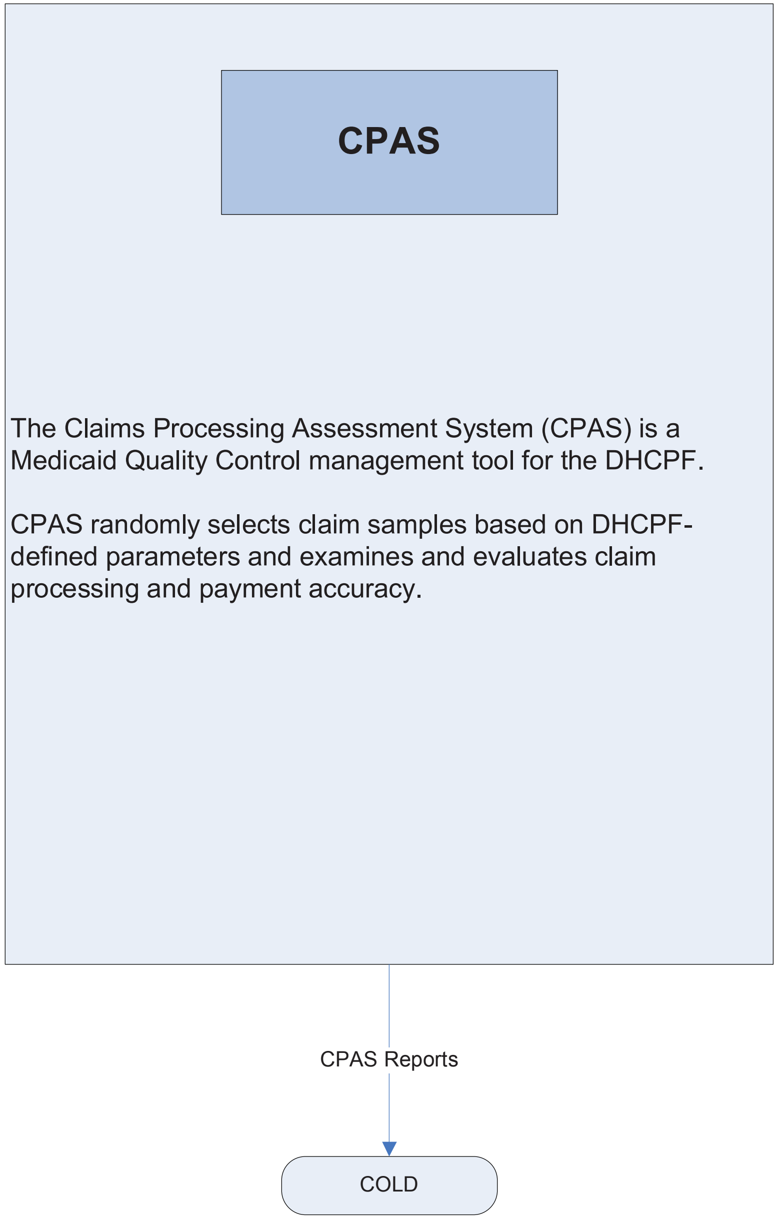
SUR provides extensive capabilities for peer grouping, data reduction and summarization, exception processing and report content control.

SUR Reports

COLD

From ACS Medicaid
Processing Overview
11/07/2008 pg 22

MMIS Back End



CPAS

The Claims Processing Assessment System (CPAS) is a Medicaid Quality Control management tool for the DHCPF.

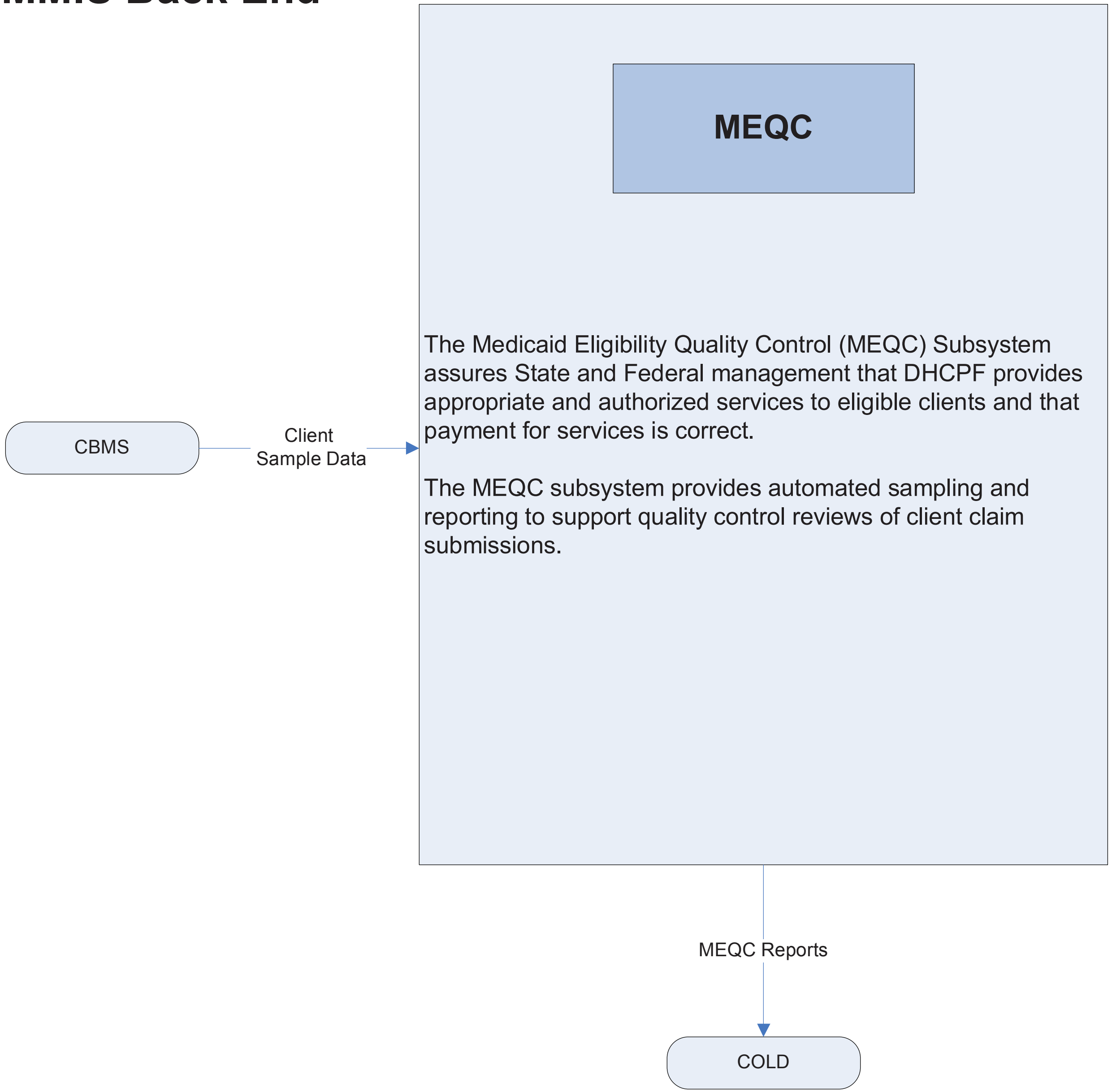
CPAS randomly selects claim samples based on DHCPF-defined parameters and examines and evaluates claim processing and payment accuracy.

CPAS Reports

COLD

From ACS Medicaid
Processing Overview
11/07/2008 pg 23

MMIS Back End

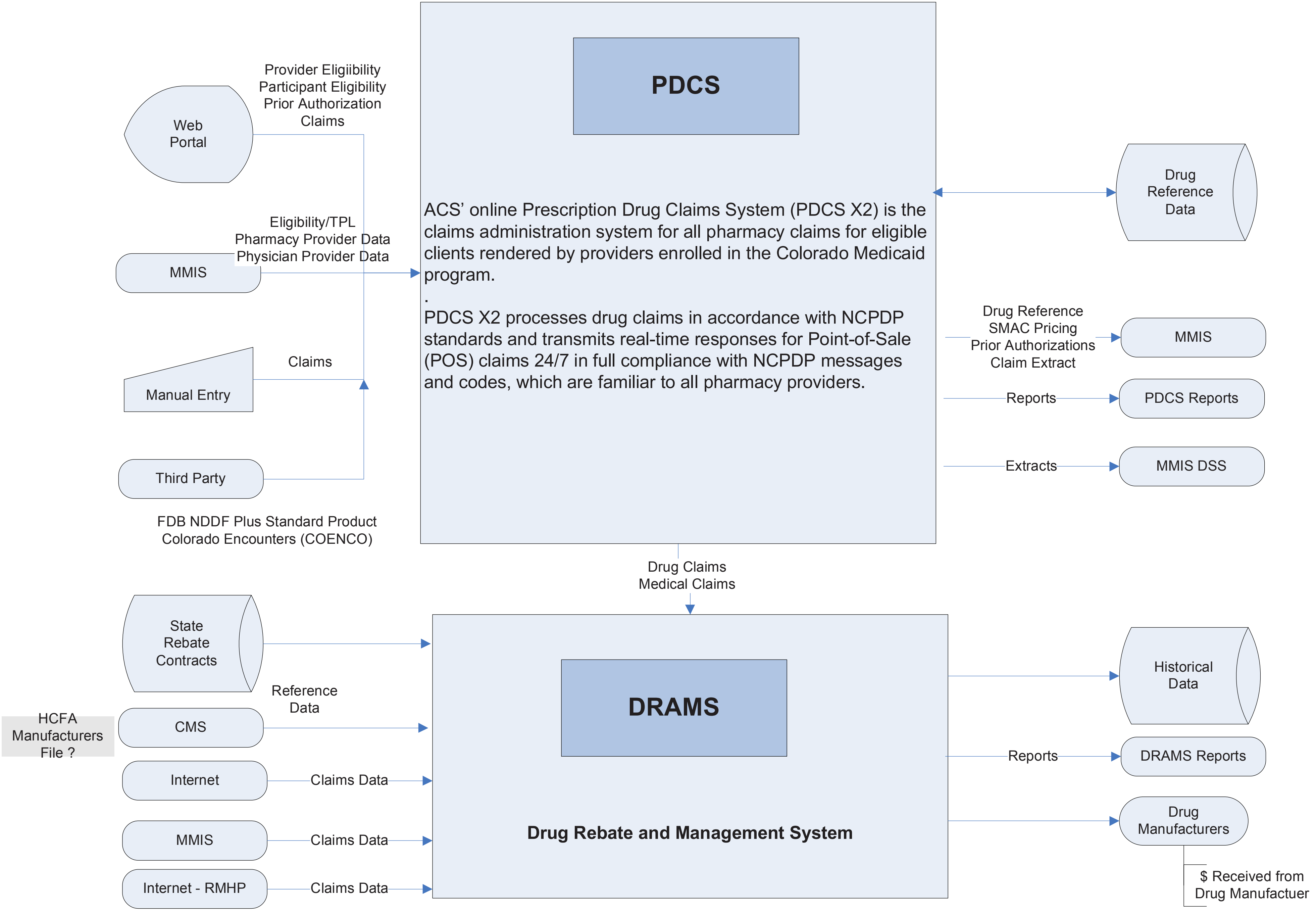


The Medicaid Eligibility Quality Control (MEQC) Subsystem assures State and Federal management that DHCPF provides appropriate and authorized services to eligible clients and that payment for services is correct.

The MEQC subsystem provides automated sampling and reporting to support quality control reviews of client claim submissions.

From ACS Medicaid
Processing Overview
11/07/2008 pg 24

MMIS Pharmacy



ACS' online Prescription Drug Claims System (PDCS X2) is the claims administration system for all pharmacy claims for eligible clients rendered by providers enrolled in the Colorado Medicaid program.

.

PDCS X2 processes drug claims in accordance with NCPDP standards and transmits real-time responses for Point-of-Sale (POS) claims 24/7 in full compliance with NCPDP messages and codes, which are familiar to all pharmacy providers.

MMIS Pharmacy

PDCS

Provider – PDCS verifies provider eligibility by matching the provider number to the information on the Provider master file. The verification insures that a particular pharmacy is eligible to provide services to members of a specific group and plan on the date of service.

Participant – PDCS verifies that the client has an active MMIS status and is authorized to receive pharmacy claim benefits on the claim's date of service. Eligibility is determined by comparing the claim date of service with the client's eligibility coverage date spans on the PDCS Eligibility file. Data on the Eligibility file is obtained directly from the MMIS Client Subsystem via the daily client eligibility interface.

Prior Auth – The Prior Authorization (PA) component insures that the client was eligible for the current plan's normally non-covered benefits on the claim's date of service. The claim date of service is compared to the client's medical profile record containing all prior authorization (PA) information.

Claims – All claims are processed according to standards set by the National Council for Prescription Drug Programs (NCPDP), version 3.2C. NCPDP provides a standardized electronic POS and batch claim submission format. Paper claims are submitted using the Colorado Pharmacy Paper Claim Form (PCF-1), which contains information that meets NCPDP and PDCS processing requirements.

Cust-Group-Plan – The Plan Custom Screen is an online record of drug coverage override parameters within a specific plan for Colorado Medicaid. Group is the eligibility group to which the participant belongs. Plan identifies under which plan the participant is eligible.

Reference – PDCS receives drug reference updates weekly from First DataBank. The PDCS provides a daily prior authorization (PA) file and a weekly reference file to the MMIS. Benefit limits and parameters are established on the Plan and Drug Reference files.

General – The Prescription Drug Card System (PDCS) is a stand-alone point-of-sale (POS) prescription drug claim processing system. The system includes online, real-time Prospective Drug Utilization Review (DUR) for claims submitted directly from a pharmacy provider via telecommunication. Prescription drug claims are directly entered into the PDCS through the exam entry function (paper claims) or in batch mode through an Electronic Data Interchange interface.

MMIS Pharmacy

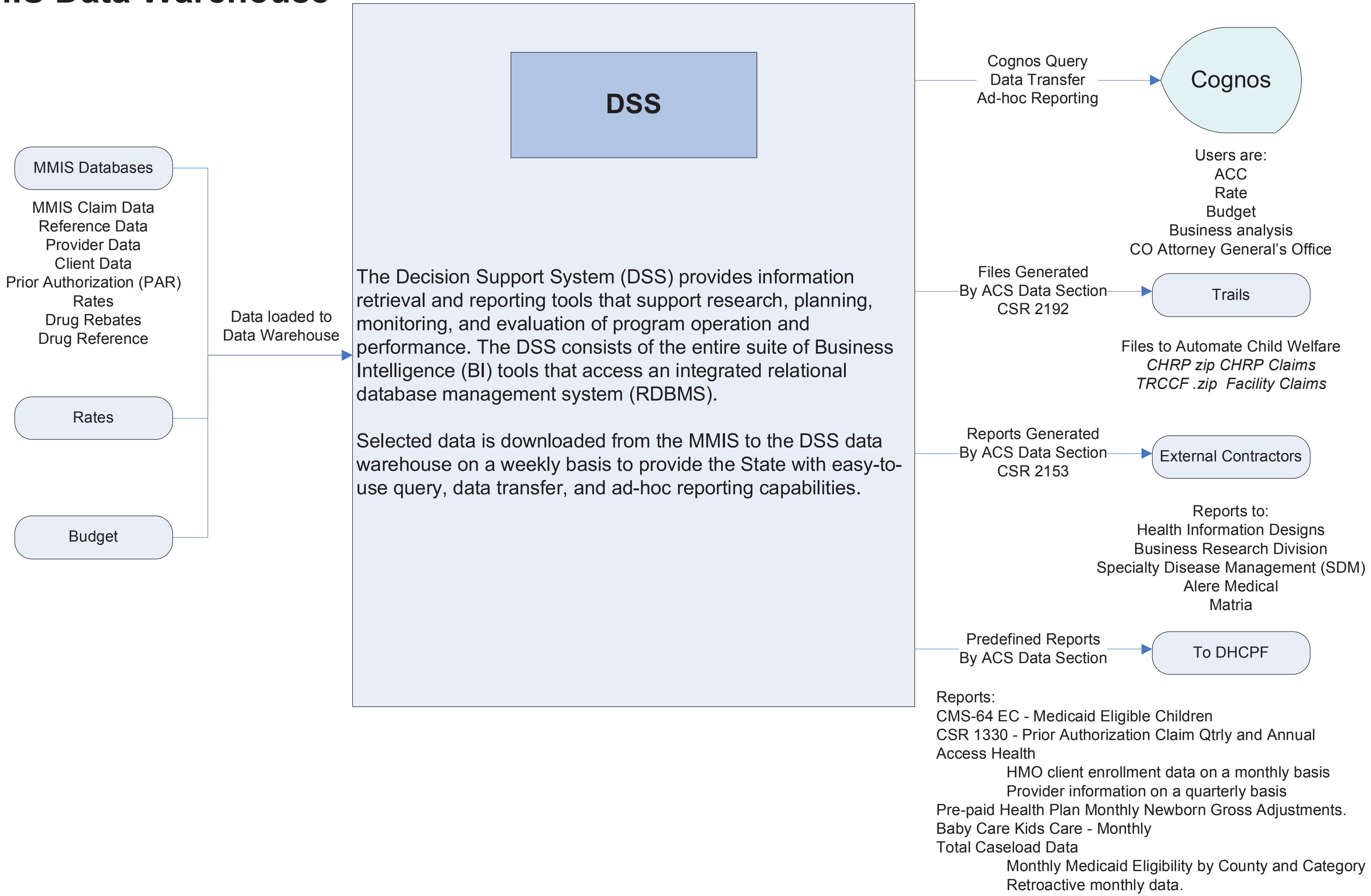
DRAMS

The ACS Drug Rebate Analysis and Management System (DRAMS) ensures compliance with the Centers for Medicare and Medicaid Services (CMS) Drug Rebate program, established under OBRA 90. Under the Drug Rebate Program, Colorado Medicaid recovers cash rebates from drug manufacturers whose products are used by Colorado Medicaid clients. The DRAMS tracks pharmacy claims for drugs and professional billed medical claims and invoices drug manufacturers using drug information and rebate amounts specified by CMS and stated amounts in approved State Supplemental Rebate contracts.

DRAMS supports multiple rebate schedules for healthcare programs and a payment reconciliation function. The DRAMS system extracts claim data for paid pharmacy claims from the Reporting Repository system to prepare invoices for rebate amounts due which are then submitted directly to pharmaceutical manufacturers.

The DRAMS application generates quarterly Drug Rebate invoices for the State and sends them to drug manufacturers. The DRAMS also maintains drug manufacturer information, records the remittance advices received from manufacturers with their rebate payments, and tracks manufacturers’ adjustments and disputes, and dispute resolution. Each quarter, the DRAMS application creates invoices in addition to Collection and Dispute Resolution Letters. These letters are produced whenever a manufacturer has not paid all of what is due for an invoice.

MMIS Data Warehouse



MMIS Claim Data
Reference Data
Provider Data
Client Data
Prior Authorization (PAR)
Rates
Drug Rebates
Drug Reference

The Decision Support System (DSS) provides information retrieval and reporting tools that support research, planning, monitoring, and evaluation of program operation and performance. The DSS consists of the entire suite of Business Intelligence (BI) tools that access an integrated relational database management system (RDBMS).

Selected data is downloaded from the MMIS to the DSS data warehouse on a weekly basis to provide the State with easy-to-use query, data transfer, and ad-hoc reporting capabilities.

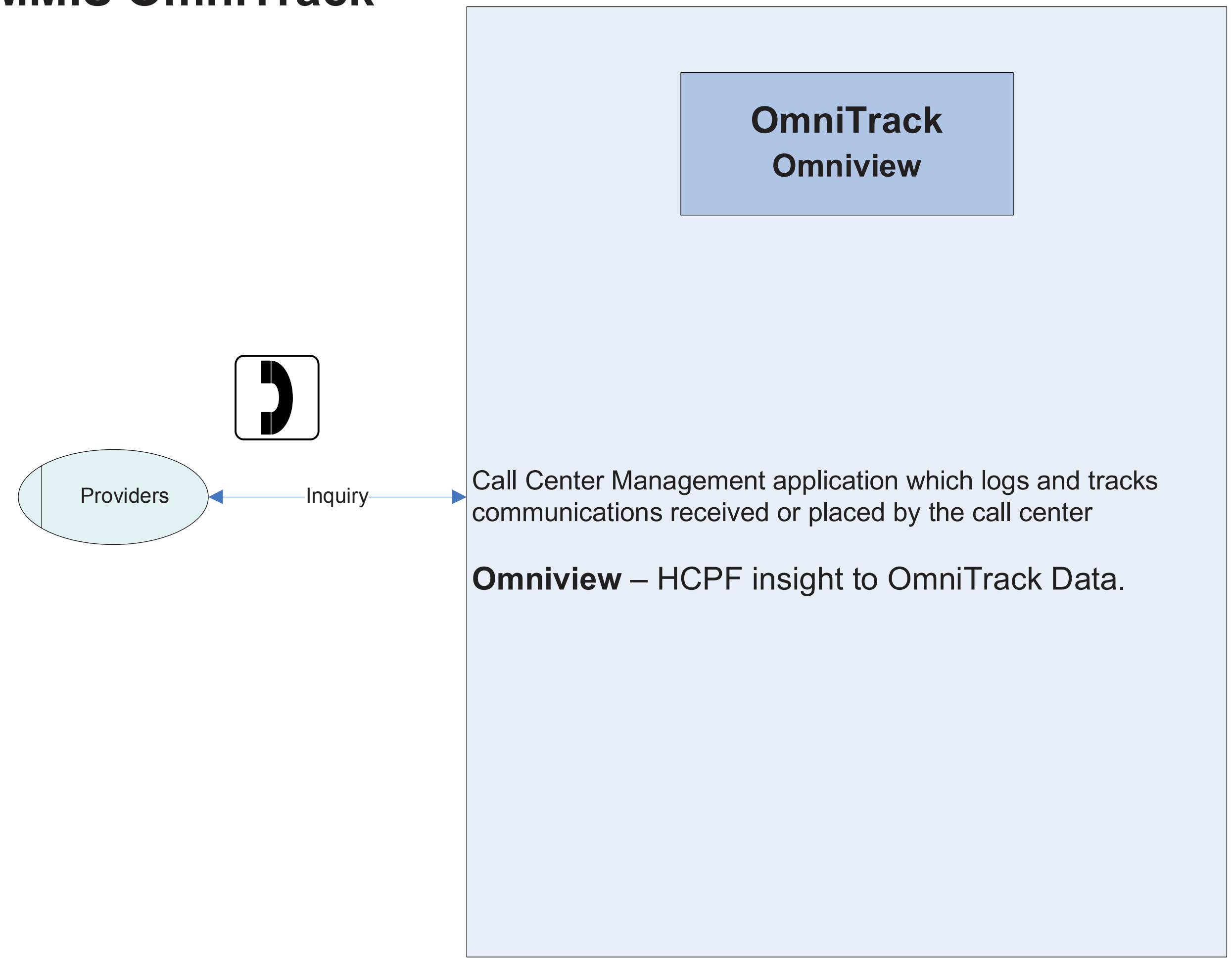
Users are:
ACC
Rate
Budget
Business analysis
CO Attorney General's Office

Files to Automate Child Welfare
CHRP zip CHRP Claims
TRCCF .zip Facility Claims

Reports to:
Health Information Designs
Business Research Division
Specialty Disease Management (SDM)
Alere Medical
Matria

Reports:
CMS-64 EC - Medicaid Eligible Children
CSR 1330 - Prior Authorization Claim Qtrly and Annual
Access Health
    HMO client enrollment data on a monthly basis
    Provider information on a quarterly basis
Pre-paid Health Plan Monthly Newborn Gross Adjustments.
Baby Care Kids Care - Monthly
Total Caseload Data
    Monthly Medicaid Eligibility by County and Category
    Retroactive monthly data.

MMIS OmniTrack



Call Center Management application which logs and tracks communications received or placed by the call center

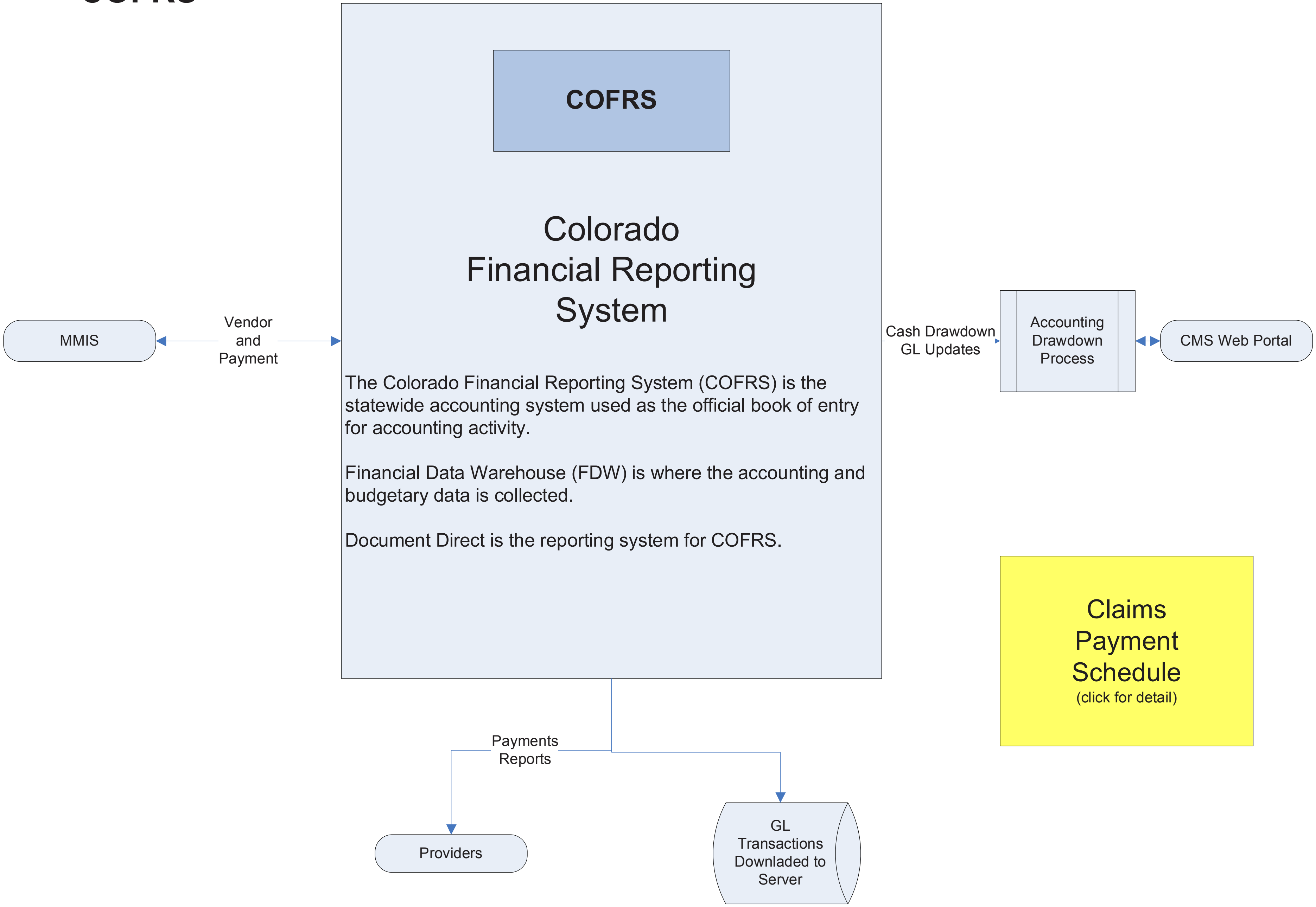
Omniview – HCPF insight to OmniTrack Data.

The Interaction Tracking system (**OmniTrack**) is a call center management application which logs and tracks communications received or placed by the call center. The OmniTrack application's primary function is logging and tracking communications made between the FAS and providers. The primary users are those within the call center that receive calls or place calls to a provider or provider group who need to track and manage correspondences required to resolve open issues.

OmniTrack integrates with the call center phone system and automatic call distribution facilities to assist call center operators when an incoming call is routed to the operator. The system uses Computer Telephony Integration (CTI) to pass a Medicaid provider number or National Provider Identifier (NPI) of the caller to OmniTrack. OmniTrack automatically retrieves and presents demographic data and a list of previous contracts in a 'screen pop' window, without requiring the operator to enter the caller identification.

OmniTrack provides user tools to format and produce standard outbound correspondence from forms created as Microsoft Word templates. Templates can be created and maintained by call center users using Microsoft Word on their own workstations, without requiring programming support.

COFRS


COFRS
Colorado Financial Reporting System
MMIS
Vendor and Payment
Cash Drawdown GL Updates
Accounting Drawdown Process
CMS Web Portal
Payments Reports
Providers
GL Transactions Downloaded to Server

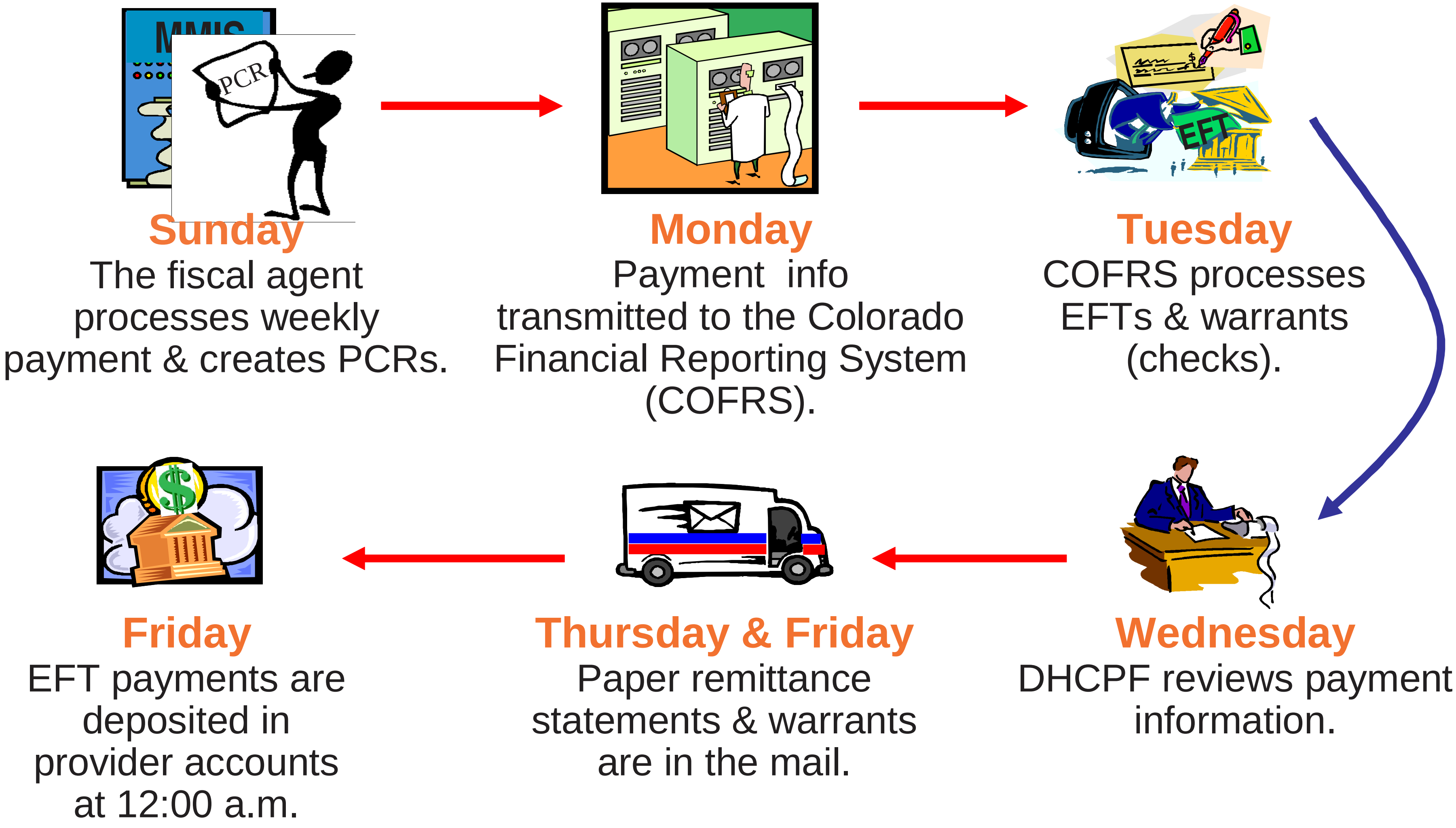
The Colorado Financial Reporting System (COFRS) is the statewide accounting system used as the official book of entry for accounting activity.

Financial Data Warehouse (FDW) is where the accounting and budgetary data is collected.

Document Direct is the reporting system for COFRS.

Claims Payment Schedule
(click for detail)

Claims Payment Schedule



Sunday
The fiscal agent processes weekly payment & creates PCRs.

Monday
Payment info transmitted to the Colorado Financial Reporting System (COFRS).

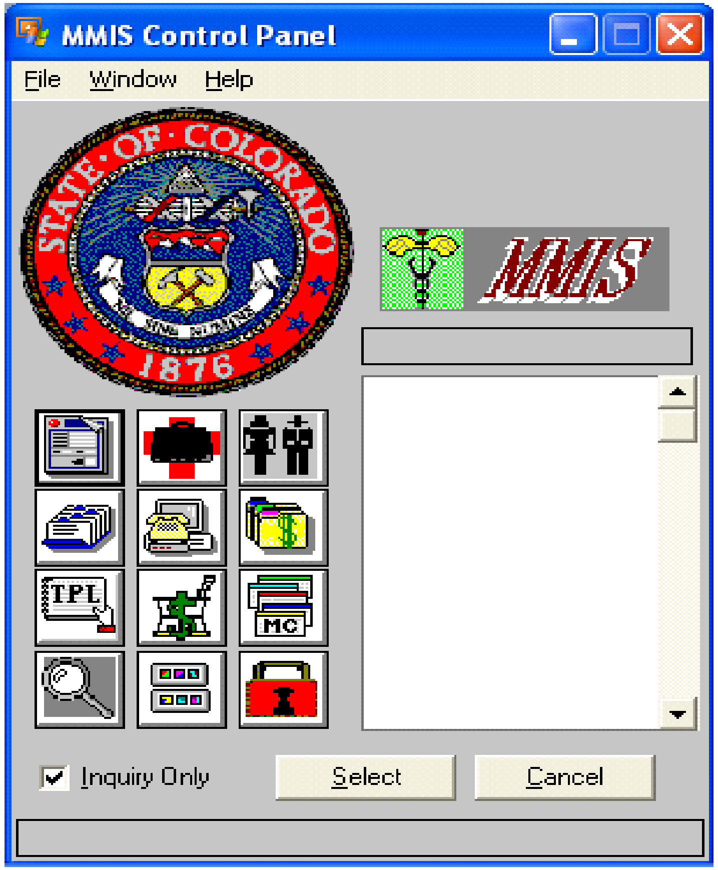
Tuesday
COFRS processes EFTs & warrants (checks).

Wednesday
DHCPF reviews payment information.

Thursday & Friday
Paper remittance statements & warrants are in the mail.

Friday
EFT payments are deposited in provider accounts at 12:00 a.m.

This document is ACS Proprietary and Confidential



MMIS Control Panel

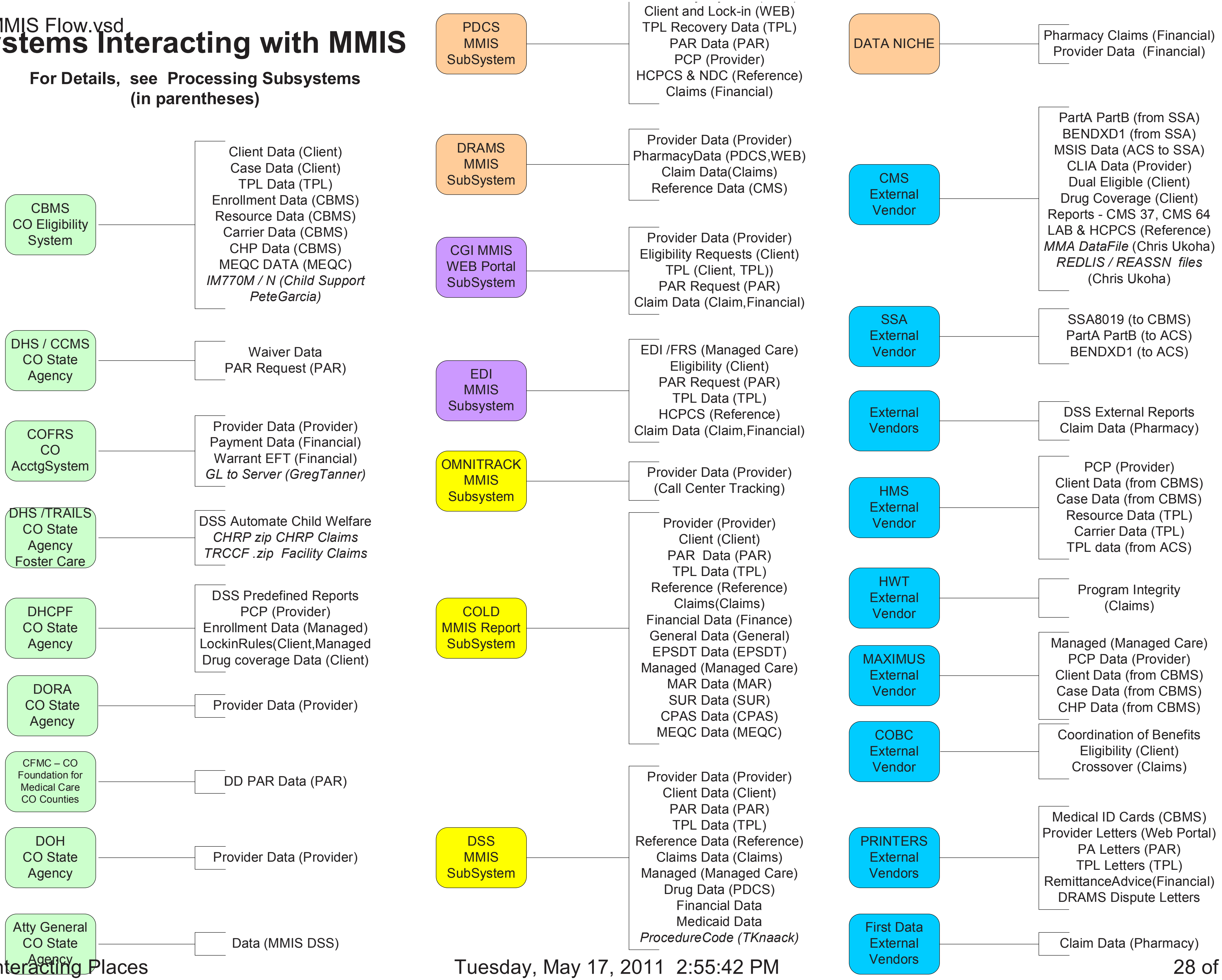
☑ Inquiry Only

MMIS “Bingo” Card – Icon Descriptions

Claim	Provider	Client
Reference	Authorization	Rates
TPL	Drug Rebate	Managed Cate
SUR	Other EPDST, MEQC CPAS, Locking System Paramters andLists	Security

Systems Interacting with MMIS

For Details, see Processing Subsystems (in parentheses)



CBMS CO Eligibility System
- Client Data (Client)
- Case Data (Client)
- TPL Data (TPL)
- Enrollment Data (CBMS)
- Resource Data (CBMS)
- Carrier Data (CBMS)
- CHP Data (CBMS)
- MEQC DATA (MEQC)
- *IM770M / N (Child Support PeteGarcia)*

DHS / CCMS CO State Agency
- Waiver Data
- PAR Request (PAR)

COFRS CO AcctgSystem
- Provider Data (Provider)
- Payment Data (Financial)
- Warrant EFT (Financial)
- *GL to Server (GregTanner)*

DHS /TRAILS CO State Agency Foster Care
- DSS Automate Child Welfare
- *CHRP zip CHRP Claims*
- *TRCCF .zip Facility Claims*

DHCPF CO State Agency
- DSS Predefined Reports
- PCP (Provider)
- Enrollment Data (Managed)
- LockinRules(Client,Managed
- Drug coverage Data (Client)

DORA CO State Agency
- Provider Data (Provider)

CFMC – CO Foundation for Medical Care CO Counties
- DD PAR Data (PAR)

DOH CO State Agency
- Provider Data (Provider)

Atty General CO State Agency
- Data (MMIS DSS)

PDCS MMIS SubSystem
- Client and Lock-in (WEB)
- TPL Recovery Data (TPL)
- PAR Data (PAR)
- PCP (Provider)
- HCPCS & NDC (Reference)
- Claims (Financial)

DRAMS MMIS SubSystem
- Provider Data (Provider)
- PharmacyData (PDCS,WEB)
- Claim Data(Claims)
- Reference Data (CMS)

CGI MMIS WEB Portal SubSystem
- Provider Data (Provider)
- Eligibility Requests (Client)
- TPL (Client, TPL))
- PAR Request (PAR)
- Claim Data (Claim,Financial)

EDI MMIS Subsystem
- EDI /FRS (Managed Care)
- Eligibility (Client)
- PAR Request (PAR)
- TPL Data (TPL)
- HCPCS (Reference)
- Claim Data (Claim,Financial)

OMNITRACK MMIS Subsystem
- Provider Data (Provider)
- (Call Center Tracking)

COLD MMIS Report SubSystem
- Provider (Provider)
- Client (Client)
- PAR Data (PAR)
- TPL Data (TPL)
- Reference (Reference)
- Claims(Claims)
- Financial Data (Finance)
- General Data (General)
- EPSDT Data (EPSDT)
- Managed (Managed Care)
- MAR Data (MAR)
- SUR Data (SUR)
- CPAS Data (CPAS)
- MEQC Data (MEQC)

DSS MMIS SubSystem
- Provider Data (Provider)
- Client Data (Client)
- PAR Data (PAR)
- TPL Data (TPL)
- Reference Data (Reference)
- Claims Data (Claims)
- Managed (Managed Care)
- Drug Data (PDCS)
- Financial Data
- Medicaid Data
- *ProcedureCode (TKnaack)*

DATA NICHE
- Pharmacy Claims (Financial)
- Provider Data (Financial)

CMS External Vendor
- PartA PartB (from SSA)
- BENDXD1 (from SSA)
- MSIS Data (ACS to SSA)
- CLIA Data (Provider)
- Dual Eligible (Client)
- Drug Coverage (Client)
- Reports - CMS 37, CMS 64
- LAB & HCPCS (Reference)
- *MMA DataFile* (Chris Ukoha)
- *REDLIS / REASSN files* (Chris Ukoha)

SSA External Vendor
- SSA8019 (to CBMS)
- PartA PartB (to ACS)
- BENDXD1 (to ACS)

External Vendors
- DSS External Reports
- Claim Data (Pharmacy)

HMS External Vendor
- PCP (Provider)
- Client Data (from CBMS)
- Case Data (from CBMS)
- Resource Data (TPL)
- Carrier Data (TPL)
- TPL data (from ACS)

HWT External Vendor
- Program Integrity (Claims)

MAXIMUS External Vendor
- Managed (Managed Care)
- PCP Data (Provider)
- Client Data (from CBMS)
- Case Data (from CBMS)
- CHP Data (from CBMS)

COBC External Vendor
- Coordination of Benefits
- Eligibility (Client)
- Crossover (Claims)

PRINTERS External Vendors
- Medical ID Cards (CBMS)
- Provider Letters (Web Portal)
- PA Letters (PAR)
- TPL Letters (TPL)
- RemittanceAdvice(Financial)
- DRAMS Dispute Letters

First Data External Vendors
- Claim Data (Pharmacy)

Introduction

The processing of transactions by the Colorado Medicaid program requires the integration of a number of applications to accommodate all of the program's business requirements.

Electronic Data Interchange (EDI) – The primary EDI function represents a clearinghouse that serves as a gateway or Electronic Data Sharing Gateway (EDSG) providing mediation and routing services for inbound and outbound data exchanges.

BUS - Online information management system used by Case Managers to document all aspects of a prospective or active client's case

Medicaid Management Information System (MMIS) – The primary MMIS function is as an Online Transaction Processor (OLTP) for non-pharmacy healthcare claims and related transactions providing transaction-oriented services such as data entry, real-time processing (editing, auditing, and adjudication), and retrieval.

Prescription Drug Claims System (PDCS) – The primary PDCS function is as an Online Transaction Processor (OLTP) for pharmacy claims and related transactions providing transaction-oriented services such as data entry, real-time processing (editing, auditing, and adjudication), and retrieval.

Decision Support System (DSS) – The primary DSS function is as an Online Analytical Processor (OLAP) providing ad hoc reporting and analysis capabilities on Colorado Medicaid program data and information.

OmniTrack – The primary OmniTrack function is as an interaction tracking and workflow solution for the Fiscal Agent call center representatives to track provider inquiries and requests.

Drug Rebate and Management System (DRAMS) – The primary DRAMS function is as an invoice and letter generation and invoice tracking solution to support the recovery of rebate funds from drug manufacturers for the Colorado Medicaid program.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Electronic Data Interchange (EDI)

The EDI System is ACS' solution for processing and responding to HIPAA mandated transactions: 837, 835, 824, 820, 270/271, 276/277, 278, 997.

EDI allows client eligibility information through a FaxBack system and an Automated Voice Response System (AVRS).

EDI maintains a HIPAA Transaction compliance check system and interacts directly with the State's Web Portal through the Colorado Submission Services (CSS) processor to process claims interactively.

EDI also accepts batch submission of claims and eligibility requests and posts reports to the File Retrieval System (FRS). The FRS is the repository of provider-retrievable files and reports accessible to a submitter's using their Trading Partner ID. Submitters can retrieve their Provider Claim Reports, Claims Accepted and Rejected reports, client eligibility response, claim status response, PAR request response, and other provider information

All electronically submitted non-Pharmacy claims are handled by EDI Gateway Services Division of ACS. EDI provides submitter enrollment in the electronic claim submission program (Trade Partner Agreement) services, host computers to receive claims and retrieve electronic remittance advices. The Colorado Fiscal Agent (FAS) EDI call center provides EDI report retrieval and telephone support to assist submitters and providers with various aspects of electronic claim submission.

The EDI application handles the receipt of transactions, translation of ANSI ASC X12N standard formats to and from Colorado MMIS Internal Record Layouts (IRLs), transaction processing, and the delivery of transaction responses to submitters. The EDI application receives valid HIPAA transactions from Trading Partners (providers, billing services, and Medicare carriers and intermediaries).

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Electronic Data Interchange (EDI) Subsystem Summary – Part 1

The MMIS Electronic Data Interchange (EDI) Subsystem is the front end of the MMIS online transaction processor (OLTP). EDI electronically captures provider claims, client eligibility requests and claim status requests via a variety of methods.

The EDI Subsystem is comprised of the following components:

- Medical Electronic Verification System (MEVS)
- MMIS EDI Host Bulletin Board System (BBS) / ASAP Host Communication System (submission)
- MMIS Intranet File and Reporting System (FRS) (report retreival)
- Web portal Interactive transactions

These systems allow providers to electronically submit and retrieve MMIS information. Each is discussed separately below.

Medical Electronic Verification System (MEVS)

The Medical Electronic Verification System (MEVS) interfaces electronic claim transactions with the MMIS OLTP. This system is the central processing system for interactive and batch claim transactions as well as eligibility verifications.

Colorado Medicaid Eligibility Response System – AVRS/ CMERS is an automated voice response system that provides Medicaid eligibility, provider warrant and claim status information to providers who cannot access these functions through the interactive software or who do not have a fax machine.

Fax-Back is a phone number providers call to have an eligibility report automatically sent to the provider’s fax machine.

MMIS EDI Host Bulletin Board System (BBS) / ASAP Host Communication System

The MMIS EDI Host Bulletin Board System (BBS) / ASAP Host Communication System receives and logs batch file transmissions.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Electronic Data Interchange (EDI) Subsystem Summary – Part 2

MMIS Intranet File Reporting System (FRS)
The MMIS Intranet FRS System is the repository of provider-retrievable files and reports.
Provider Claim Reports, Claims Accepted and Rejected reports, client eligibility response, claim status response, PAR request response, and other provider information are retrievable by the submitter.

Web Portal
The Web Portal is a web-based claim entry and submission system that interactively submits ANSI X12N 837 claims, 270 Client Eligibility Request, 276 Claim Status Request, and 278 PAR Request transactions to the MMIS. The web portal also includes the reports to the FRS, EDI ECC reports and Par inquiry.

Web Portal Interactive Processing
Eligibility inquiries
Ability to search for a list of specific providers enrolled in the MMIS
Reporting features include claim status, eligibility accept/reject reports, Claims accept/reject/adjustment reports and PAR responses.
Inquire on or update demographic, Medicare ID, affiliation information, and NPI information that is stored in the MMIS.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Medicaid Management Information System (MMIS)

The Colorado MMIS is the claims administration system for all non-pharmacy healthcare claims for eligible clients rendered by providers enrolled in the Colorado Medicaid program. The MMIS online system has a Graphical User Interface (GUI), the business logic is developed in a frontend tier 4th generation rules language and a backend tier common procedural business coding language (i.e., COBOL), and the backend data storage employs a Relational Database Management System (RDBMS).

The MMIS is logically grouped into the following three areas:

Front End
Claims Processing
Back End

These three logical areas are introduced in the following paragraphs.

Front End

The Front End includes the Provider, Client, Prior Authorization, Third Party Liability, and Reference Subsystems. The Front End subsystems are used primarily to maintain the data used in claims processing. This information includes provider-related data, client-related data, and reference data. It also includes the information needed to prior authorize services, and data that is used to ensure that Medicaid is the payer of last resort through Third Party Liability (TPL) processing. Data for these subsystems typically originates outside of the MMIS and therefore these subsystems include many interfaces. This data supports the accurate and thorough processing of Medicaid claims.

Provider – The Provider Subsystem maintains current and historical provider information and allows access to provider information through online, real-time inquiry and update capabilities. The subsystem includes medical and non-medical providers and managed care plans that are eligible to participate in the DHCPF Medical Assistance Program.

Client – The Client Subsystem is the source of all client eligibility and demographic data for the MMIS. The subsystem supports an interface with the Colorado Benefits Management System (CBMS) to receive client information and to return a limited amount of non-CBMS client data regarding copay, enrollment, and disenrollment activity.

Prior Auth – The Prior Authorization (PA) Subsystem collects and maintains comprehensive current and historical PA information. The subsystem's online, real-time inquiry and update capabilities enable maintenance of and access to PA information.

TPL – The Third Party Liability (TPL) Subsystem maintains comprehensive current and historical information to support the benefit recovery functions of the MMIS. The DHCPF uses this information to reduce its payment liability for Medicaid client claims.

Reference – The Reference Subsystem provides a reliable, flexible means to maintain information required by the MMIS. The primary function of the reference database is to serve as the repository of data required for claims processing, prior authorization and third-party liability (TPL) processing.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Medicaid Management Information System (MMIS)

Claims Processing

The Claims Processing Subsystem is organized into Claims Entry, Claims Pricing and Adjudication, and Claims Financial and Reporting functionality. The Claims Entry function accepts claims into the system in a format that the system is prepared to process.

The Claims Pricing and Adjudication function edits, prices, audits, and adjudicates each claim. The Claims Financial and Reporting functions interact with the State's COFR System to reimburse the provider. This function also produces reports about claims processing, from both an operational and a financial perspective.

Claims – The Claims Processing Subsystem consists of claims entry and claims pricing and adjudication. Claims Entry includes online, real-time inquiry and update capabilities to collect and maintain claim information. Claims Pricing and Adjudication validates claims submitted by the Colorado Medicaid provider community and determines the claim's Medicaid allowed reimbursement amount.

Payment – The Claims Financial and Reporting function processes all Medicaid claims, credits, adjustments, and financial transactions through the final payment process. The subsystem produces financial and balancing reports and maintains the on-line and archived claims history database. The subsystem maintains provider financial summary information that includes tracking financial transactions that result in the establishment and maintenance of provider accounts receivable data.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Medicaid Management Information System (MMIS)

Back End

The Back End functions include the General, Early and Periodic Screening, Diagnosis, and Treatment (EPSDT), Management and Administrative Reporting (MAR), Surveillance and Utilization Review (SUR), Claims Processing Assessment System (CPAS), and Medicaid Eligibility Quality Control (MEQC) Subsystems. These reporting functions satisfy State and Federal reporting requirements.

Managed care functionality is fully integrated within the MMIS and managed care functions are included in many of the subsystems noted above. Managed care functions are accommodated in part by the addition of specific functionality to other subsystems. Other functionality resides in the Managed Care Subsystem itself.

General – The MMIS includes the entry and maintenance of system parameters and system lists, as well as the maintenance of locked records. The System Parameter function allows authorized users to enter a new parameter or search for existing parameters based on parameter number or subsystem. The System List is similar to System Parameters, but allows the user to enter start/end values and supports an unlimited range of values for each of the five allowable effective dates.

EPSDT – The Early and Periodic Screening, Diagnosis, and Treatment (EPSDT) Subsystem maintains EPSDT client demographic and screening information. The EPSDT Subsystem supports client participation in the EPSDT Program and maintains security and control over all client EPSDT-related data through DHCPF-defined function and screen level security.

Managed Care – The Managed Care Subsystem provides the DHCPF with valuable tools to help improve access to quality care. The subsystem assures the appropriate utilization of services, enhances client and provider satisfaction and achieves these in a cost efficient manner.

MARS – The MMIS Management and Administrative Reporting (MAR) Subsystem supports the administration of the Colorado Medicaid Program by providing information to the DHCPF staff responsible for program management and oversight. The MAR cycle provides monthly management reporting and summarizes and maintains data to support quarterly, semi-annual, annual and on-request reporting.

SURS – The Surveillance and Utilization Review (SUR) Subsystem creates a comprehensive statistical profile of provider delivery of health care services and supplies and client utilization of these services and supplies. SUR provides extensive capabilities for peer grouping, data reduction and summarization, exception processing and report content control.

CPAS – The Claims Processing Assessment System (CPAS) is a Medicaid Quality Control management tool for the DHCPF. CPAS randomly selects claim samples based on DHCPF-defined parameters and examines and evaluates claim processing and payment accuracy.

MEQC – The Medicaid Eligibility Quality Control (MEQC) Subsystem assures State and Federal management that DHCPF provides appropriate and authorized services to eligible clients and that payment for services is correct. The MEQC subsystem provides automated sampling and reporting to support quality control reviews of client claim submissions.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Prescription Drug Claims System (PDCS)

ACS' online Prescription Drug Claims System (PDCS X2) is the claims administration system for all pharmacy claims for eligible clients rendered by providers enrolled in the Colorado Medicaid program. The PDCS online system has a GUI (i.e., Java/J2E), the business logic is developed in a middle tier Object Oriented programming language (i.e., Java/Enterprise Java Beans) and a backend tier common procedural business coding language (i.e., COBOL), and data storage employs both a middle tier and a backend tier RDBMS (i.e., Oracle and DB2).

PDCS X2 processes drug claims in accordance with NCPDP standards and transmits real-time responses for Point-of-Sale (POS) claims 24/7 in full compliance with NCPDP messages and codes, which are familiar to all pharmacy providers. Enhanced messaging capabilities for DUR and other edits are also fully supported.

Provider – PDCS verifies provider eligibility by matching the provider number to the information on the Provider master file. The verification insures that a particular pharmacy is eligible to provide services to members of a specific group and plan on the date of service.

Participant – PDCS verifies that the client has an active MMIS status and is authorized to receive pharmacy claim benefits on the claim's date of service. Eligibility is determined by comparing the claim date of service with the client's eligibility coverage date spans on the PDCS Eligibility file. Data on the Eligibility file is obtained directly from the MMIS Client Subsystem via the daily client eligibility interface.

Prior Auth – The Prior Authorization (PA) component insures that the client was eligible for the current plan's normally non-covered benefits on the claim's date of service. The claim date of service is compared to the client's medical profile record containing all prior authorization (PA) information.

Claims – All claims are processed according to standards set by the National Council for Prescription Drug Programs (NCPDP), version 3.2C. NCPDP provides a standardized electronic POS and batch claim submission format. Paper claims are submitted using the Colorado Pharmacy Paper Claim Form (PCF-1), which contains information that meets NCPDP and PDCS processing requirements.

Cust-Group-Plan – The Plan Custom Screen is an online record of drug coverage override parameters within a specific plan for Colorado Medicaid. Group is the eligibility group to which the participant belongs. Plan identifies under which plan the participant is eligible.

Reference – PDCS receives drug reference updates weekly from First DataBank. The PDCS provides a daily prior authorization (PA) file and a weekly reference file to the MMIS. Benefit limits and parameters are established on the Plan and Drug Reference files.

General – The Prescription Drug Card System (PDCS) is a stand-alone point-of-sale (POS) prescription drug claim processing system. The system includes online, real-time Prospective Drug Utilization Review (DUR) for claims submitted directly from a pharmacy provider via telecommunication. Prescription drug claims are directly entered into the PDCS through the exam entry function (paper claims) or in batch mode through an Electronic Data Interchange interface.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Decision Support System (DSS)

The Decision Support System (DSS) provides information retrieval and reporting tools that support research, planning, monitoring, and evaluation of program operation and performance. The DSS consists of the entire suite of Business Intelligence (BI) tools that access an integrated relational database management system (RDBMS). Selected data is downloaded from the MMIS to the DSS data warehouse on a weekly basis to provide the State with easy-to-use query, data transfer, and ad-hoc reporting capabilities.

The DSS online system employs a “ zero footprint” thin client GUI using standard Internet browsers, business logic is developed within report and data queries using the Business Intelligence (BI) query and report design tools, and data storage employs a backend tier RDBMS (i.e., Oracle).

The DSS databases include MMIS claim data, as well as reference, provider, client, and prior authorization data. The Oracle databases are updated by weekly downloads from the MMIS DB2 database on the ACS Government Healthcare Solutions mainframe. The DSS BI tools applications are robust, flexible query and reporting tools that allow users access to detail and summarized data for ad-hoc queries, analysis, and reporting.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

OmniTrack

The Interaction Tracking system (OmniTrack) is a call center management application which logs and tracks communications received or placed by the call center. The OmniTrack application's primary function is logging and tracking communications made between the FAS and providers. The primary users are those within the call center that receive calls or place calls to a provider or provider group who need to track and manage correspondences required to resolve open issues.

The OmniTrack online system employs a GUI (i.e., PowerBuilder), business logic resides within the online windows and database procedures and triggers, and data storage employs a backend tier RDBMS (i.e., Sybase).

OmniTrack integrates with the call center phone system and automatic call distribution facilities to assist call center operators when an incoming call is routed to the operator. The system uses Computer Telephony Integration (CTI) to pass a Medicaid provider number or National Provider Identifier (NPI) of the caller to OmniTrack. OmniTrack automatically retrieves and presents demographic data and a list of previous contracts in a 'screen pop' window, without requiring the operator to enter the caller identification.

OmniTrack provides user tools to format and produce standard outbound correspondence from forms created as Microsoft Word templates. Templates can be created and maintained by call center users using Microsoft Word on their own workstations, without requiring programming support.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Drug Rebate and Management System (DRAMS)

The ACS Drug Rebate Analysis and Management System (DRAMS) ensures compliance with the Centers for Medicare and Medicaid Services (CMS) Drug Rebate program, established under OBRA 90. Under the Drug Rebate Program, Colorado Medicaid recovers cash rebates from drug manufacturers whose products are used by Colorado Medicaid clients. The DRAMS tracks pharmacy claims for drugs and professional billed medical claims and invoices drug manufacturers using drug information and rebate amounts specified by CMS and stated amounts in approved State Supplemental Rebate contracts.

The DRAMS online system employs a GUI (i.e., PowerBuilder), business logic resides within the online windows and database procedures and triggers, and data storage employs a backend tier RDBMS (i.e., Oracle).

DRAMS supports multiple rebate schedules for healthcare programs and a payment reconciliation function. The DRAMS system extracts claim data for paid pharmacy claims from the Reporting Repository system to prepare invoices for rebate amounts due which are then submitted directly to pharmaceutical manufacturers.

The DRAMS application generates quarterly Drug Rebate invoices for the State and sends them to drug manufacturers. The DRAMS also maintains drug manufacturer information, records the remittance advices received from manufacturers with their rebate payments, and tracks manufacturers’ adjustments and disputes, and dispute resolution. Each quarter, the DRAMS application creates invoices in addition to Collection and Dispute Resolution Letters. These letters are produced whenever a manufacturer has not paid all of what is due for an invoice.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Computer Output to Laser Disk (COLD) Storage and Retrieval System

ACS uses eSystems LANPATH Report Manager as the Computer Output to Laser Disk (COLD) storage and retrieval system for the Colorado MMIS. Report Manager enables the storage, indexing, and viewing of multiple high-volume reports in an electronic format. The COLD solution is an efficient replacement for microfiche.

All production reports are available through COLD. For each report, the user accesses the report by name and version (the date that the report was generated). Also, within specific reports, certain fields are set up as indexes. For example, a user can select the provider number index on the Provider Claim Report to call up the data for a particular provider, instead of paging through the entire report. The user is also able to search on a text string within a report.

Authorized users have an icon on their workstation desk top that allows them to enter Report Manager. Since these reports are centrally stored on a shared network, multiple users can access the same report simultaneously.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Other Systems used by HCPF Personnel

(based on Security Access Request Forms)

OIT DocFinity

OIT DocFinity is the electronic capture and management system of documents to include secure web access to the image repository.

Systematic Alien Verification for Entitlements (SAVE)

The SAVE system determines immigration status information required for determining a non-citizen applicant’s eligibility for many public benefits.

CBMS

The Colorado Benefits Management System is used by the counties and Medical Assistance Sites to determine Program eligibility. Default access includes inquiry access to alerts, scanning, traffic log, case comments, client referral, application intake, interactive interview, case assignment, eligibility, authorization, redetermination, eligibility spans, and medical ID card requests.

CBMS-DSS (COGNOS)

The CBMS Decision Support System contains report data taken from the CBMS.

The source of much of this information (but not all) is from the ACS Stateshare folder:
Z:\Maintenance\System Doc\ < there is a folder per subsystem, and
Z:\Audits and Audit Support\MMIS Statewide Audit\CUST-20081002 Medicaid Processing Overview.pdf

Other Files for HCPF Personnel

(Interface Programmer intervention needed for User Access)

E.CBMS.MMIS.IM770M and E.CBMS.MMIS.IM770N - download MF to PC
files are for Child Support – send to Pete Garcia – loads to Access DB

X.UHA.M.COPRCIN - download MF to PC
Procedure codes – send to Theresa Knaak – (could use DSS instead, but needs more fields)

X.HCPF.BUYIN.CDCO.REASSN.Dyymmdd.Txxxxxxx
800 x 18400 ~13,000 records Annual ~Oct 15 and Nov 15
Files for Chris Ukoha – had an Access DB, Greg Donlin put file in .xls format and forwaded to user (couldn't find Access DB)

X.HCPF.BUYIN.CDCO.REDLIS.Dyymmdd.Txxxxxxx
600 x 27600 ~4,500 records Annual ~Sept 15
Files for Chris Ukoha – had an Access DB, Greg Donlin put file in .xls format and forwaded to user (couldn't find Access DB)

E.CBMS.CMS.DATAFILE (also, see DATAFIX and MMACOPD)
180 x 27900 ~350,000 records Monthly ~16th
CBMS sends this file to CMS - CMS dataset received is: P#DDP.#DDP3.CMS.IN.ELIGIBLE.CO
Greg converts data to Access db, puts on O drive and sends a note to Chris Ukoha (Pharmacy section) that the file is there

E.CBMS.CMS.DATAFIX.G0035V00 (also, see DATAFILE and MMACOPD)
180 x 27900 ~210,000 records Monthly ~20th
CBMS sends this file to CMS - P#EFT.IN.ELIGIBLE.CMSCO.D100920.T1159428
Used in the Phasedown report

X.HCPF.BUYIN.MMACOPD(0) (also, see DATAFILE and DATAFIX) - where is this file used ? in CBMS ?
3400 x 27200 ~196,000 records Monthly ~21st
The 1st 180 characters is the E.CBMS.CMS.DATAFILE, the rest is the CMS updates

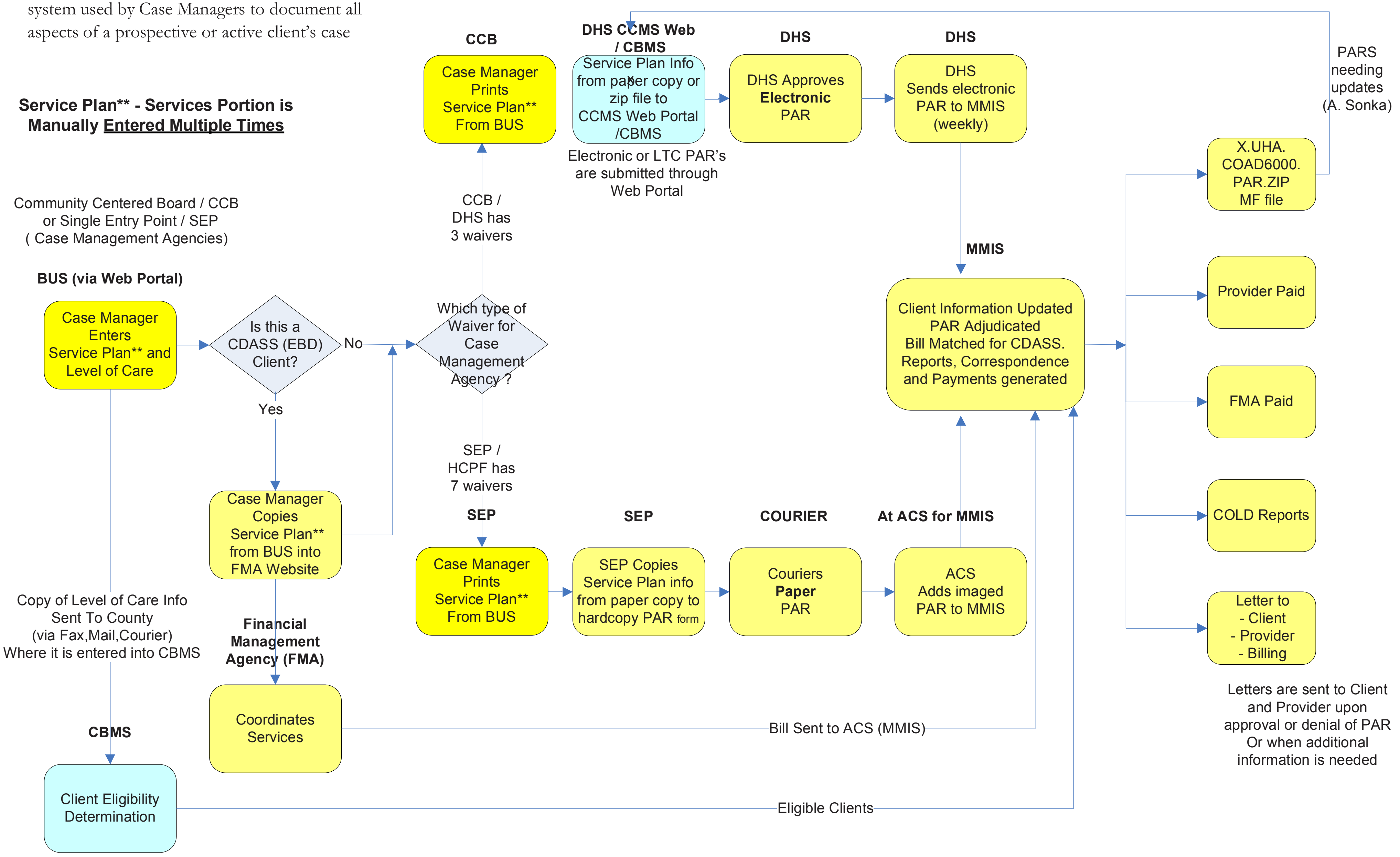
X.HCPF.CMS.LIS(0) -where is this file used ?
350 x 27650 ~25,000 records Monthly ~ 10th

X.UHA.M.MANCTPL -where is this file used ?
I believe this is from ACS Monthly ~1st

LTC PAR data into MMIS

BUS - Online information management system used by Case Managers to document all aspects of a prospective or active client’s case

Service Plan - Services Portion is Manually Entered Multiple Times**



Community Centered Board / CCB or Single Entry Point / SEP (Case Management Agencies)

BUS (via Web Portal)

Case Manager Enters Service Plan** and Level of Care

Is this a CDASS (EBD) Client?

No

Yes

Case Manager Copies Service Plan** from BUS into FMA Website

Financial Management Agency (FMA)

Coordinates Services

Bill Sent to ACS (MMIS)

Copy of Level of Care Info Sent To County (via Fax,Mail,Courier) Where it is entered into CBMS

CBMS

Client Eligibility Determination

Eligible Clients

Which type of Waiver for Case Management Agency ?

CCB / DHS has 3 waivers

CCB

Case Manager Prints Service Plan** From BUS

DHS CCMS Web / CBMS

Service Plan Info from paper copy or zip file to CCMS Web Portal /CBMS

Electronic or LTC PAR’s are submitted through Web Portal

DHS

DHS Approves **Electronic** PAR

DHS

DHS Sends electronic PAR to MMIS (weekly)

MMIS

Client Information Updated PAR Adjudicated Bill Matched for CDASS. Reports, Correspondence and Payments generated

SEP / HCPF has 7 waivers

SEP

Case Manager Prints Service Plan** From BUS

SEP

SEP Copies Service Plan info from paper copy to hardcopy PAR form

COURIER

Couriers **Paper** PAR

At ACS for MMIS

ACS Adds imaged PAR to MMIS

PARS needing updates (A. Sonka)

X.UHA. COAD6000. PAR.ZIP MF file

Provider Paid

FMA Paid

COLD Reports

Letter to
- Client
- Provider
- Billing

Letters are sent to Client and Provider upon approval or denial of PAR Or when additional information is needed

Q – CFMC is a CCB or SEP?

Office of Information Technology

{System Name}

System Security Plan

{DATE}

This document contains confidential information for OIT Official Use Only. It shall not be duplicated, used, or disclosed in whole or in part without prior written permission from the Information Security Staff.

Table of Contents

1 System Record of Changes

Issue	Date	Pages Affected	Description
Template Origination	May-14,2012	All	Initial Draft Version 1.1

1.1 Instructions on Completing the Template

- Text in **BLUE** are text insertions that need to be responded to by the writer of the plan.
- Texts in BLACK are standard template text that are required to be included in the Security Plan and should not be deleted unless necessary.
- Discussion text in **RED** are included to assist in the writer with the development of responses, provide consistency in responses necessary to fulfill the requirements for that section. Discussion text should be deleted after the section has been completed but may be left there for future reference if desired.
- Response Examples in **RED** are also provided in many sections as content reference. Example text should be deleted after the section has been completed to prevent any reader confusion.

1.2 Record of Changes

Modifications made to this plan, since the last printing, are listed on the Change Information Page contained in this document.

2 System Architecture Plan Objectives

2.1 Introduction

The purpose of a System Architecture Plan (SAP) is to provide an overview of [System Name] information system security requirements and identify any State, National or Federal security controls in place or planned to meet security requirements. The SSP also delineates responsibilities and expected behavior of all individuals who own, access or manage the information system and should be viewed as documentation of the structured process for planning adequate, cost-effective security protection for a major application or general support system. It should reflect input from various managers with responsibilities concerning the information system, including information owner(s), system owner(s), system operator(s), and the information security officers. Additional information may be included in the basic plan, and the structure and format organized according to requirements.

The security plan provides documentation of the structured process for managing and monitoring the information system to ensure the confidentiality, integrity and availability of the system. Components of each SSP include a system classification, risk assessment, environmental architecture design documentation, disaster Recovery plans, system interdependencies document and regulatory security requirements section. It reflects input from management responsible for the system, including information owners, the system operator, the system security manager, and system administrators. The System Architecture Plan delineates responsibilities and expected behavior of all individuals who access the system.

Each System Architecture Plan is developed in accordance with the guidelines contained in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, Guide for Developing Security Plans for Information Technology Systems, and applicable risk mitigation guidance and standards.

Summarized in each plan are all security findings that indicate weaknesses in each system and recommended security controls that need to be corrected to ensure system compliance to State, National and Federal laws.

Documented in this plan are findings that indicate weaknesses in [System Name] security controls that need to be corrected. These findings are summarized as follows and will be tracked in the Colorado Risk Incident and Security Compliance (CRISC) system until corrected:

Discussion: After completing the security assesment for the system summarize any findings that are considered high risk or high vulnerability to the system here. The intention of this summary is to identify any security finding that poses a risk to the system prior to being implemented into a production environment. ALL items identified in this section must be added to the Colorado Risk Incident and Security Compliance (CRISC) system, and mitigation plans to correct security findings will be developed, implemented and validated for compliance to identified security standards identified in this document. **(This section should match the information developed from the System Security Control Plan)**

- Identify here each significant risk finding. [Example: Lack of Identification and Authentication.]
- Identify here each significant risk finding.
- Identify here each significant risk finding.

3 Intended Audience

This document is designed to be used by those parties responsible for managing and/or creating the SSP for an individual general support system or minor/major business application. System owners are organizationally responsible for conducting these activities; however, guidance and implementation assistance is frequently provided at an organizational level. Within OIT, guidance to complete the SSP, as well as support for the activities associated with, is provided by the Security Policy and Compliance Section.

4 System Identification

4.1 System Name / Title

Discussion:
Enter the System Name and acronym given to the general support system or application.

4.2 System Owner – Agency Contacts

The designated person(s) have sufficient knowledge of the system to be able to provide additional information or points of contact regarding the security plan and the system, as needed. They are the decision making authority as to budgetary and operation function of the system or solution

Discussion: Specify the program owner, program manager and the system manager to contact for further information regarding the security plan and the system. Include their address, telephone numbers, and e-mail. List the name, title, organization, and telephone number of one or more persons designated to be the point(s) of contact for this system. The contacts given should be identified as the system owner, program manager, and system manager. The designated persons should have sufficient knowledge of the system to be able to provide additional information or points of contact, as needed.

System personnel contacts include contact information for the system owner, authorizing official, other designated contacts, and the division security officer.

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

4.3 Responsible Organization – Data Owner

The data owner is the designated individual who is ultimately responsible for the confidentiality, Integrity and Availability (CIA) of the data owned by the System Owner. This individual typically determines how data is accessed, who the data is accessed by, its distribution and security. This individual has a clear understanding of all state, national, federal or international laws and regulations governing the security and access of the data.

Discussion: In this section, list the organization that owns and is responsible for the data in the application. The responsible organization owns the system, the data it contains, and controls the use of the data. List the federal organizational sub-component responsible for the system. If a state or local government or contractor performs the function, identify both the federal and other organization and describe the relationship. Be specific about the organization and do not abbreviate. Include phone numbers, physical locations, and addresses.

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

4.4 Agency Chief Information Officer (CIO)

The Agency Chief Information Officer is the designated person responsible for the general management of the IT system or solution utilized by a system owner or agency. This Individual is the decision making authority over budgetary requirements, project design, disaster recovery and ongoing maintenance and support of the system or solution for the system owner or agency.

List the Agency Chief Information Officer (CIO) or other person(s) responsible for the development, integration and ongoing IT support of an IT solution used by the system owner / agency, including their address and phone number. To be effective, this individual must be knowledgeable of the management, operational, and technical controls used to protect the system owners IT solution or system. You may also want to consider developing or amending an existing Service Level Agreement (SLA) to define the CIO to system owner relationship and service expectations for the respective system being developed on maintained at the agency.

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

4.5 Agency Information Security Officer (ISO)

The designated person(s) responsible for the security of the system has been assigned responsibility in writing to ensure that the [GSS or Major Application] has adequate security and is knowledgeable of the management, operational, and technical controls used to protect the system.

Discussion: List the Information Security Officer (ISO), or other person(s) responsible for the security of the system, including their address and phone number. An individual must be assigned responsibility to ensure that the GSS or Major Application has adequate security. To be effective, this individual must be knowledgeable of the management, operational, and technical controls used to protect the system. Include the name, title, and telephone number of the individual who has been assigned responsibility for the security of the system. You may also want to consider sending a memorandum from the organizational manager (or equivalent) to the person (or persons) identified in the SSP as responsible for security to officially confirm their appointment. If a memorandum is done, be sure to include a signed copy with the SSP.

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

4.6 System Subject Matter Expert / Administrator

The Subject Matter Expert (SME) is the individual responsible for the overall management and administration of the system. This individual is involved in all technical discussions for the system to include access control, documentation, applications, hardware, data, design and Disaster Recovery requirements for the system and is the primary contact for all security events affecting the system.

List the primary subject matter expert responsible for the overall support and technical administration of the IT system or solution identified in this SSP, or other person(s) responsible for the management of any vendor supported system or solution , including their address and phone number. This individual must be knowledgeable of the management, operational, and technical controls used to protect the system and any SLA requirements in place for the system or solution. Include the name, title, and telephone number of the individual below .

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

4.7 Authorizing Official

The Colorado Chief Information Security Officer (CISO) after review of each System Architecture Plan (SSP) is the individual responsible for sponsoring and approving the operation or denying operation of state computing systems and solutions for the state of Colorado.

Discussion: The authorizing official is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals. The authorizing official has the following responsibilities related to System Architecture Plans:

- Approves System Architecture Plans,
- Authorizes operation of an information system,
- Issues an interim authorization to operate the information system under specific terms and conditions, or
- Denies authorization to operate the information system (or if the system is already operational, halts operations) if unacceptable security risks exist.

Name:		**Address:**	
Title:		**Phone**	
Agency:		**E-mail**	

5 General System Description and Purpose of the System

Discussion: Present a brief description (one to three paragraphs) of the function and purpose of the system (e.g., economic indicator, network support for an organization, business census data analysis, and crop reporting support). Be sure to include the type(s) of information that the GSS or Major Application processes. If the system is a major application, describe and provided a data flow diagram. If the system is a general support system, list all applications supported by the general support system. Specify if the application(s) is or is not a major application and include unique name/identifiers, where applicable. Describe each application's function and the information processed. Include a list of user organizations pertaining to this system, whether they are internal or external to the system owner's organization, and a general description of the type of information and processing provided. Request information from the application owners (and a copy of the security plans for major applications) to ensure their requirements is met.

Example: The ABC LAN is the communication system, which is designed to facilitate the services and resources needed to support the operations of ABC's users. The ABC LAN supports several minor applications. Appendix B Minor Application Inventory Form provides minor application description, categorization, user community and responsible organization.

6 System Mission Criticality

Discussion:
The system owner, ISO and CIO will collaborate to determine the Mission Critical prioritization for the system or General Support Infrastructure based on the 5 prioritization baselines listed below. Once a system is prioritized, the CIO and system Subject Matter Expert (SME) will provide a detailed Disaster Recovery Plan (DRP) which meets the prioritization classification requirements for the system. The Completed DRP should be attached to this System Architecture Plan.

Example:
The state criminal history system is considered a Priority 1, Mission Critical core business system for the state of Colorado. An outage to this system would cause significant business impact to most all state agencies increase likelihood of loss of life or irreparable damage to operations, staff or citizens could occur.

{Insert copy of the supporting Disaster Recovery Plan Here}

Priority 1 – Instant Failover and Redundancy

Required for those essential state services that must maintain minimal to no service disruption. Typically, these systems are categorized as mission critical or essentilal core state systems whose functions provide support for mission critical operations and are dependencies for other applications or services to be recovered. If systems are not sustained, critical operations within the federal, state County and municipal governmental agencies cease to exist and the liklihood of loss of life or irreparable damage to operations, staff or citizens could occur. The recovery strategy for Priority 1 systems is a “redundant” or “instant” failover strategy where redundant systems are currently deployed in an alternate recovery facility or facilities.

Priority 2 – Hot Recovery - (8 hour recovery window)

Required for those core services that must be maintained with limited service disruption. Typically, these systems provide support for mission critical operations and are dependencies for other applications or services to be recovered. If systems are not sustained, loss of life or irreparable damage to operations, staff or citizens could occur. The recovery strategy for Priority 2 systems is a “Hot” strategy where redundant systems are currently deployed in an alternate recovery facility.

Priority 3 – Warm Recovery - (48 hour recovery window)

Required for those systems and data where service disruption will cause serious injury to government operations, staff or citizens. Typically, these systems and applications service required to support emergency operations and delivery of core government operations. The recovery strategy for Priority 3 systems will typically be a “Warm” strategy. Systems will be deployed in an alternate recovery facility but data is not installed and systems are not routinely maintained at a level where failover operations would be seamless.

Priority 4 – Warm/Cold Recovery - (<5) Business Days

Required for moderately critical agency services and IT functions where damage to government operations, staff and citizens would be significant but not serious. Typically, these systems support services that are provided by the agency in a non-emergency environment.
Depending on the type of system and ease of system replication, a “Warm” or “Cold” recovery strategy could be selected. In a cold recovery process, systems would be acquired form remote state inventories or purchased on an emergency basis from a reliable vendor at the time a disaster is declared. However, the acquisition of replacement systems would have to be defined in a reasonable process to ensure availability of the required systems. This may require a contract for standby equipment.

Priority 5 – Cold Recovery - (>5) Business Days

Required for less critical support systems. In many cases, these systems would not be deployed at the alternate recovery sties. The Priority 5 systems may be restored in primary operating site a few weeks after the primary disaster has dissipated. The most common recovery strategy for Priority 5 systems is a “Cold” strategy. No standby agreements are deployed and the state is at risk that systems are no longer available or that

7 System Classification

All State systems must be classified based on the type of information that is available within the system and to external sources. The classification of every system is based on the Confidentiality, Integrity and Availability of the system information to the end user.

7.1 Classification of Asset Based On Risk Evaluation (CARE)

Discussion: Use the Office of Information Security (OIS) Classification of Asset based on Risk Evaluation (CARE) system Spreadsheet to classify this system and include the completed CARE document as an attachment to this document. Once the system is classified all identified security controls for the operation of the system must be incorporated into the system security score card. Based on the outcome of the CARE scorecard, enter your results in the table below.

	Confidentiality	**Integrity**	**Availability**
Cumulative Impact Level	ADD YOUR RATING HERE	ADD YOUR RATING HERE	ADD YOUR RATING HERE
FIPS 199 Categorization	**Moderate**		

7.2 General Description of Information Sensitivity

In accordance with Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems, information categorization is calculated based on the three basic security objectives: confidentiality, integrity, and availability. NIST Publication 800-60 Guide for Mapping Types of Information and Information System to Security Categories provides implementation guidance in completing this activity.

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. ***Systems that contain Personal Identifiable Information (PII) may not be low for confidentiality and must be either a moderate or high.***	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals. ***Systems that contain Personal Identifiable Information (PII) may not be low for integrity and must be either a moderate or high.***	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

7.3 System Information Handled

Discussion: This section provides a description of the types of information handled by the system, an analysis of the sensitivity of the information stored within, processed by, or transmitted by a system and appropriate background investigation required for access.

The description will provide information to a variety of users, including: Analysts/programmers who will use it to help design appropriate security controls; Internal and external auditors evaluating system security measures; managers making decisions about the reasonableness of security countermeasures; and users accessing the system including system administrators, database administrators and/or application support staff members completing the appropriate background investigation forms.

Sensitivity levels range from low to high based on the type(s) of information processed

- Determine the sensitivity level of the information based on the information in Exhibits 1 and 2. Systems that contain Personal Identifiable Information (PII) are automatically either a moderate or high level sensitivity.
- Indicate the overall system sensitivity level by using the highest data sensitivity level from the table.
- Described the nature of the information sensitivity and criticality.
- Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system.
- If applicable describe information on applicable laws, regulations, and policies affecting the system and a general description of sensitivity.

Example: HIGH RISK - The ABC System is the primary communications network that supports ABC's users in their day-to-day operations. This information system is continuously used during business and non-business hours, supporting many businesses processing within the agency's computing environment. The confidentiality, integrity and availability of the ABC system is critical, i.e., ensuring that data is only received by the persons and applications that it is intended for, that data is not subject to unauthorized or accidental alterations, and that the resources are available when needed. Due to the sensitivity of this information system, all personnel with system administration rights and roles will required an elevated background investigation to fulfill their duties.

8 System Environment – Architecture

8.1 Infrastructure Details

Discussion: Provide a brief (one-three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns, such as:

- The system is connected to the Internet;
- It is located in a harsh or overseas environment;
- Software is rapidly implemented; The software resides on an open network used by the general public or with overseas access;
- The application is processed at a facility outside of the organization's control; or
- The general support mainframe has dial-up lines.

Describe the primary computing platform(s) used (e.g., mainframe, desktop, Local Area Network (LAN) or Wide Area Network (WAN)). Include a general description of the principal system components, including hardware, software, and communications resources. Provide server names and IP addresses. Discuss the type of communications included (e.g., dedicated circuits, dial circuits, public data/voice networks, Internet). Describe controls used to protect communication lines in the appropriate sections of the security plan.
Include any security software protecting the system and information.

Describe in general terms the type of security protection provided (e.g., access control to the computing platform and stored files at the operating system level or access to data records within an application). Include only controls that have been implemented or are planned, rather than listing the controls that are available in the software. Controls that are available, but not implemented, provide no protection.

Specify any system components that are essential to its operation, but that are not included within the scope of the plan, and the reason that this is so (i.e., covered under another plan, etc.).
Lastly, insert the system architecture diagram in this section after the text description.

Example: The ABC system is housed in a government owned building in Washington, DC. The entire building is occupied by the Department of Housing and Urban Development and contractor personnel and is not open to the general public. The ABC LAN operates Microsoft NT, version 4.0, and workstations run Windows 95. The security software protecting all system resources is the built in security of Microsoft Windows NT. The ABC LAN supports all office automation applications for ABC. The ABC LAN has dial up lines from each subordinate site. Users are required to be authenticated with user ID and password before access is granted to the network. Additionally, a personal firewall and up-to-date antivirus software is installed on each user's machine prior to the laptop being issued for travel.

[Insert System Architecture Diagram Here]

9 System Interconnection / Information Sharing Dependencies

Discussion: System interconnection is the direct connection of systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and information sharing and the increased controls required to mitigate those vulnerabilities. The security plan for the systems often serves as a mechanism to affect this security information exchange and allows management to make informed decisions regarding risk reduction and acceptance.

A description of the rules for interconnecting systems and for protecting shared data must be included with this security plan.

In this section, provide the following information concerning the authorization for the connection to other systems (including the internet) or the sharing of information:

List of interconnected systems (including Internet);

- Unique system identifiers, if appropriate;
- Name of dependent or connected system(s);
- Organization owning the other system(s);
- Type of interconnection (TCP/IP, Dial, SNA, etc.);
- Name and title of authorizing management official(s);
- Date of authorization;
- System of Record, if applicable (Privacy Act data);
- Sensitivity level of each system;
- Interaction among systems; and
- Security concerns and Rules of Behavior of the other systems that need to be considered in the protection of this system.

Example: The ABC LAN is interconnected with County backbones for Internet and Intranet access. The ABC LAN is a level II system and the information within the ABC LAN is currently shared with other state and county networks, and other Federal agencies for the sharing of Protected Health Information (PHI). Business Associate agreements exist between counties 1-65 and the Colorado Department of Health and Human Services. Contracts are maintained but the Office of Information Security for the state of Colorado and have been executed and by legal and are on file with the ISSO. The Rules of Behavior have to be read, understood, and signed by each user. This system is a Level one (1) high Security system and is required to meet federal HIPAA/HITECH security controls as defined in the Security Scorecard for level 1 systems of this type and sensitivity. Connections between state ancd County entities are TCP connections using secured VPN tecnologies to ensure secure communications. Web access utilizes SSL certificates from trusted host, Entrust and is a non-expiring certificate.

10 Applicable Laws or Regulations Affecting the System

Discussion: List any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of data/information in this specific application. Each organization should decide on the level of laws, regulations, and policies to include in the security plan. Examples might include the Privacy Act or a specific statute or regulation concerning the information processed (e.g., tax or census information). If the system processes records subject to the Privacy Act, include the number and title of the Privacy Act system(s) of records and whether the system(s) are used for computer matching activities.
See the NIST Computer Security Division's Computer Security Resource Clearinghouse (CSRC) Web site for additional information (http://csrc.nist.gov).

Example:

This section shows the Federal laws, regulatory guidance, and directives that drive the essential security controls for the (System Name Here) system

- Federal Information Security Management Act (FISMA) of 2002
- HIPAA/HITECH security act 164.x security requirements
- Computer Fraud and Abuse Act of 1986, as amended.
- Privacy Act of 1987
- Federal Information Processing Standard 199 –
- NIST SP 800-18 Rev. 1 - Guide for Developing Security Plans for Federal Information Systems, February 2006
- NIST SP 800-30 - Risk Management Guide for Information Technology Systems, July 2002
- NIST SP 800-34 - Contingency Planning Guide for Information Technology Systems, June 2002
- NIST SP 800-37 – Guide for the Security Certification and Accreditation of Federal Information Systems, May 2004
- NIST SP 800-53 Rev. 2– Recommended Security Controls for Federal Information Systems, December 2007
- NIST SP 800-60 Volume I and II- Guide for Mapping Types of Information and Information Systems to Security Categories, June 2004

List individual contracts executed for accessing or sharing information if needed here Ie HIPAA Business associate agreements!

Section G5.0

Annual Colorado MMIS Claim Volume

State Fiscal Year	Annual Claim Volume*
FY 2007-08	21,599,362
FY 2008-09	28,947,869
FY 2009-10	26,228,518
FY 2010-11	28,706,577
FY 2011-12	34,268,869
FY 2012-13	38,000,000
FY 2013-14	45,900,000
FY 2014-15	54,000,000
FY 2015-16	57,300,000
FY 2016-17	59,000,000
FY 2017-18	59,900,000
FY 2018-19	60,100,000
FY 2019-20	60,300,000
FY 2020-21	60,500,000
FY 2021-22	61,000,000
FY 2022-23	61,600,000

*Includes paid and denied fee-for-service based claims, paid capitations, and paid encounters. FY 2007-08 through FY 2011-12 values are actuals, FY 2012-13 through FY 2022-23 values are Department estimates.

COLORADO DEPARTMENT OF HEALTH CARE POLICY & FINANCING

1570 Grant Street, Denver, CO 80203-1818 • (303) 866-2993 • (303) 866-4411 Fax • (303) 866-3883 TTY

John W. Hickenlooper, Governor • Susan E. Birch MBA, BSN, RN, Executive Director

January 25, 2013

Richard C. Allen
Associate Regional Administrator
Division of Medicaid and Children's Health Operations
Centers for Medicare and Medicaid Services
1600 Broadway, Suite 700
Denver, Colorado 80202

Subject: Provider Screening and Enrollment Regulation Implementation

Dear Mr. Allen:

This letter contains responses to the questions of your June 11, 2012 letter to the Colorado Department of Health Care Policy and Financing (Department) and formally submits for your review revised State Plan Amendment pages related to Transmittal Number 12-009. In addition, this letter incorporates informal questions and responses between the Department and your office that have occurred since the Department submitted a draft response to this RAI on September 28, 2012.

The Amendment adds item 4.46 Provider Screening and Enrollment to Section 4 of the State Plan, and describes the Department's compliance with the requirements for provider screening specified in 42 CFR §455 Subpart E (Rules). The Department is revising several sections of item 4.46.

The Department is attempting to provide a thoughtful response to the regulations and is not stating compliance with the regulation. The Department's strategy for implementation of the Provider Screening Rules of the Affordable Care Act was developed to align with its imminent procurement of a replacement Medicaid Management Information System (MMIS) including a provider enrollment system. The Department's replacement MMIS and provider enrollment system is expected to be operational by July 2016.

Several important factors played a role in the development of the Department's strategy:

1. The current MMIS is based on older technology and lacks the flexibility for rapid and cost effective implementation of new requirements.
2. The Department is in the process of replacing the current MMIS by July 2016. Implementation of the replacement MMIS and the provider enrollment system will place significant demands on the Department's staff and resources.
3. State mandated initiatives and Departmental program updates intended to expand coverage and reduce expenses as directed under the Affordable Care Act are also in progress.

"The mission of the State of Health Care Policy & Financing is to improve access to cost-effective, quality health care services for Coloradans."

As a result, neither the Department nor the Department's Fiscal Agent are staffed or funded for significant additional efforts that are not transferrable to the replacement MMIS.

In order to be compliant with the Rules as much as possible during the transition to the replacement MMIS and with its fiscal responsibilities, the Department has developed and adopted the following strategy regarding the Rules:

1. The Department will avoid system updates to the current MMIS which could be better implemented in the replacement MMIS. Because of the technology of the current MMIS, system changes are costly and require long implementation times. As a result, changes made to the current system would be in service only a short period of time and not transferrable to the replacement system, resulting in only a small return on the investment of effort. Furthermore, they would delay implementation of currently planned system upgrades intended to expand program coverage and reduce expenses.
2. The Department will avoid interim administrative and paper-based solutions where the effort is not transferrable to the replacement MMIS. This allows Department staff to focus on the longer term permanent solution and avoids expenses for 'throw away' solutions where the practical benefits are short term and limited.
3. The Department will augment or improve current administrative processes where possible to achieve increased compliance with the Rules. The provider enrollment application will be augmented and the Department will make better use of existing screening options and tools.
4. The Department will implement the tools and processes necessary to fully comply with the Rules as a first priority of the replacement MMIS and fiscal agent contract. For example, the successful responder to the RFP for the replacement MMIS is required to provide a tool for online provider enrollment (OPE) by July 2014 and to propose a plan to complete provider re-enrollment by March 2016 as required by the Rules.

The questions of your June 11, 2012 letter and our responses are as follows.

- For 42 CFR 455.410, please provide information to explain why the State is not able to enroll physicians and other professionals who order or refer services. Since the State is already enrolling providers that render and bill for services, what is the difference between a provider which only orders or refers and one which submits claims since the information required is the same for both types. As required under 42 CFR 455.440, the National Provider Identifier (NPI) of the ordering or referring provider is required on claims submitted by the provider performing the order or referred service. If the State's concern is related to the NPI requirement, please explain why the State requires 3.5 years to incorporate the NPI on the claim record. In addition, please explain why it will take 4 years to edit claims based on the NPI of the ordering or referring provider

  Response: In keeping with the strategy outlined above:

  1. The Department wishes to avoid using the relatively costly and error prone current paper/administrative process to enroll referring (only) and ordering (only)

providers. The OPE tool, to be implemented by July 2014 will allow for much more efficient enrollment of all roles of providers. (Note however, that even with the OPE tool, claims will not be systematically adjudicated for the referring or ordering NPI until after the replacement MMIS is operational in 2016.)

2. The Department wishes to avoid the extensive system updates for editing of ordering or referring provider NPIs in the current MMIS that will soon be replaced. The Department will begin editing for an ordering or referring NPI when the replacement MMIS is operational.

Note also the response to 42 CFR 455.440, below.

- Per SPA 12-009, the State is able to verify licenses today using an existing process which is acceptable from the regulatory provision perspective. If the State whishes to modify or automate this process, we are supportive of such efforts. Because the State is already in compliance with 455.412, please explain why an automated approached creates a barrier to compliance until December 2015.

  Response: The Department is indeed exploring low cost improvements in its processes for validation of the licensure of most CO providers. In the interim, the Department will rely on its current processes for provider licensure validation and is largely compliant with this rule. A common repository of downloadable provider licensure data from all states would be helpful. SPA 12-009 has been updated accordingly.

- For 42 CFR 455.416, that providers be terminated if they have been terminated by another State Medicaid/CHIP agency or by Medicare and information is currently available to assist the State with the termination process. Please explain the barriers for the State in implementing this provision.

  Response: In keeping with the strategy outlined above:

  1. The Department is largely in compliance with (a) and (b) of 42 CFR 455.416.
  2. The Department will update its provider screening processes for newly enrolling providers to comply with the enrollment requirements of part (c) by June 2013. The Department is compliant with the requirement to terminate providers terminated by Medicare or other state.
  3. The Department will include managing employees in its screening of newly enrolling providers to comply with part (d) by June 2013.

  SPA 12-009 has been updated accordingly.

- For 42 CFR 455.420, if the State does terminate providers, are these providers allowed to re-enroll after a period of time? If so, please provide additional information which explains the December 2015 implementation date for the reactivation of terminated providers.

Response: The Department is compliant with this rule with the exception of the collection of fees. The Department is researching the state statutes regarding the collection of fees. See the response for 42 CFR 455.460. SPA 12-009 has been updated accordingly.

- For 42 CFR 455.422, if the Department provides appeal rights for a provider whose request for enrollment is denied, what is the barrier to having this requirement implemented under the current process? Please provide additional information as to why the State is proposing to not implement this provision until December 2015.

  Response: The Department is currently compliant with this rule. SPA 12-009 has been updated accordingly.

- For 42 CFR 455.432, please provide information identifying the barriers the State is facing which delays conducting site visits until December 2015. This regulation does not require States to enter the results of site visits into the MMIS while we do support such modifications at the discretion of the State. The same is true for 42 CFR 455.434 which requires fingerprinting and criminal background checks and CMS will be releasing additional guidance regarding this soon.

  Response: The Department is currently compliant with this rule. The Department will establish screening levels that match the Medicare requirements under the Rules, such that all site visits will be performed according to Medicare enrollment activities prior to Medicaid enrollment. SPA 12-009 has been updated accordingly.

- For 42 CFR 455.436, the State is currently checking Federal databases within its existing provider enrollment process as indicated in your May 25, 2012 cover letter to CMS. While an automated approach is more efficient, it is not required under the regulatory provision. We need additional information as to why these Federal database checks for newly enrolling providers cannot be done until December, 2015.

  Response: The Department is largely compliant with this rule with respect to the providers themselves. The Department will update its procedures regarding the disclosure of operating managers for newly enrolling providers. Full compliance with respect to owners and managing employees for newly enrolling providers will be achieved by June 2013. Full compliance with part (c)(2) must be deferred until this data can be systematically captured by the OPE tool. SPA 12-009 has been updated accordingly.

- For 42 CFR 455.440, please explain the barrier for including the NPI for the ordering or referring provider on the claim from the provider performing the ordered or referred service.

  Response: The Department currently requires that the referring provider be identified on claims for certain procedures and clients. The NPI will be edited on these non-pharmacy claims in June 2013. Full compliance will accomplished with the implementation of the replacement MMIS and provider enrollment system by July 2016.

- For 42 CFR 455.450, what is the barrier that prohibits the State from establishing the screening levels until December 2015. The rule defines which providers are limited, moderate, or high risk provider and the screening requirements. Since the State is already performing the screening requirements for limited risk providers, why will it require 3.5 years to implement these screening requirements for moderate or high risk providers?

  Response: The Department is currently compliant with this rule. The Department will establish screening levels that match the Medicare requirements under the Rules. SPA 12-009 has been updated accordingly.

- For compliance under 42 CFR 455.460, please provide the rationale of why the State is not able to implement the collection of application fees until December 2015. Is legislation required at the State level to support this?

  Response: For 42 CFR 455.460, Department can implement this requirement through a regulation change. Legislation is not required. However, the State is subject to a state constitutional limitation on the amount of revenue that is can collect. Therefore, the Department must request an opinion from the Attorney General's Office if such revenue would be subject to that state constitutional limitation. If so, then by collecting this revenue, there is a possibility that other tax revenue collected by the state could be impacted and the Department may need to request a waiver to this requirement. At this time, the Department has not formally requested that opinion and expects that it will take more than 6-months to receive a formal response from the Attorney General's Office. In addition, the Department needs to have the new online provider enrollment (OPE) functional to understand if the provider has already paid a fee to Medicare and to provide the functionality to collect the fee. Such an operational process does not currently exist, so the fiscal controls to collect the fee are not in place. Therefore, the Department believes that the appropriate response is that this process is being researched to understand the legal ramifications on state revenues and that the Department currently plans to implement this through the new MMIS by providing a tool for online provider enrollment (OPE) by July 2014. SPA 12-009 has been updated accordingly.

- For 42 CFR 455.470, if the Secretary imposes a temporary moratorium for a specific provider type, what is the barrier for the State to not allow any new enrollments of such provider until the moratorium is over? If a request from such a provider is received, the provider would be notified that a moratorium exists and then would be notified when the moratorium has ended. Please provide additional information as to why 3.5 years are needed to implement this provision.

  Response: For 42 CFR 455.470, the Department is compliant with this rule. SPA 12-009 has been updated accordingly.

In addition, the Department is submitting the following information:

- For 455.416 on the termination of providers there is an existing system which CMS has available for States. The system includes Medicare and Medicaid termination information. The system is called Medicaid/CHIP Information Sharing Service (MCSIS). State can have multiple licenses to the system and we understand that the information can be downloaded. In addition, States enter information into the system as well. Thus, is the State of Colorado aware of MCSIS? Are you using it?

  Response: The Department uses the MCSIS data to for post-enrollment screening of providers. The Department will begin using MCSIS for pre-enrollment screening beginning no later than June 2013.

- For 455.436 even if the process is not automated the exclusion databases do allow for multiple searches. If the State is capturing owners of providers there is no reason to wait until 2016 to be utilizing the databases for enrollment. In addition, without making any modification to the existing MMIS does the State have a mechanism to extract data from the system to be used for the monthly exclusion database checks?

  Response: The Department does not currently require disclosures of managing employee data and does not record the disclosure of owner data after screening. As a result, at this time, post-enrollment screening of managing employees is not possible and post-enrollment screening of owners is not practical. Post-enrollment screening of the providers themselves is conducted by the Department monthly. Beginning June 2013, the Department will use exclusion databases for pre-enrollment screening of providers, their owners and managing employees. Beginning as soon as possible after July 2014, the databases will be used for monthly screening of recently enrolled providers, their owners and managing employees post-enrollment.

- For 455.440 is the State indicating that pharmacies do not report the NPI of the prescribing provider on the claim? If they do what action is the State able to make to review the claims with NPIs of providers not enrolled? The basis of this provision is to protect the program against significant abuses in the ordering of services like prescriptions. What actions will the State take to impact this need? Will providers be contacted if they order prescriptions and are not enrolled in order to get them to enroll? What action will the State take to investigate potential inappropriate actions by providers regarding such abuses? Is the State using a Point of Service (POS) processing environment for prescriptions? Is this environment part of the MMIS or is it separate with an interface with the MMIS? If it is separate what action within the POS could be taken to implement the changes. The point is that there are a number of actions a state could take even if they are not positioned to fully implement the claim edits into the MMIS until the new MMIS is implemented. A 2016 date before any actions to implement the provision, even if not totally implemented, is not acceptable.

> Response: The Department investigated the characteristics of recent pharmacy claims regarding this rule. It was found that about 3,800 ordering (prescribing) providers would need to be enrolled in the CO program in order to comply with the rule in addition to system changes for both the pharmacy point-of-sale system and the MMIS. The enrollment of this number of providers in the short term using the current paper-based process is impractical and would likely be disruptive for clients. As a result, the cost of system changes was not investigated further. The Department suspects that other states would have similar challenge and believes that requiring enrollment – possibly in many states – only for the purpose of prescribing adds unreasonable administrative burden to the providers.
>
> The Department will begin a campaign to enroll prescribing providers after the online provider enrollment tool is ready. Full implementation of editing of the prescribing NPIs for pharmacy claims will be implemented with the new MMIS in 2016.

The Department considers these plans regarding provider Screening and Enrollment Regulation to be a prudent use of resources during a time when many other expectations have been placed on the Department with modest increases in our operating budget. If you have any questions regarding this Amendment, please contact Chris Underwood at 303-866-4766.

Sincerely,

John Bartholomew
Director, Finance Office

STATE PLAN UNDER TITLE XIX OF THE SOCIAL SECURITY ACT

State/Territory: Colorado

4.46 Provider Screening and Enrollment (Page 1 of 3)

Citation
1902(a)(77)
1902(a)(39)
1902(kk)
P.L. 111-148 and
P.L. 111-152
	The State Medicaid agency gives the following assurances:

42 CFR 455 Subpart E	PROVIDER SCREENING __X__Assures that the State Medicaid agency complies with the process for screening providers under section 1902(a)(39), 1902(a)(77) and 1902(kk) of the Act. **The Department expects to be partially compliant with these regulations as described below and fully compliant by July 2016.**
42 CFR 455.410	ENROLLMENT AND SCREENING OF PROVIDERS __X__Assures enrolled providers will be screened in accordance with 42 CFR 455.400 et seq. __X__Assures that the State Medicaid agency requires all ordering or referring physicians or other professionals to be enrolled under the State Plan or under a waiver of the Plan as a participating provider. **The Department is largely compliant with part (a) of these regulations and expects to implement improvements by June 2013. The Department expects to begin compliance with part (b) of these regulations by July 2014 and be fully compliant by March 2016.**
42 CFR 455.412	VERIFICATION OF PROVIDER LICENSES __X__ Assures that the State Medicaid agency has a method for verifying providers licensed by a State and that such providers licenses have not expired or have no current limitations. **The Department is largely compliant with these regulations.**
42 CFR 455.414	REVALIDATION OF ENROLLMENT __X__ Assures that providers will be revalidated regardless of provider type at least every 5 years. **The Department expects to begin compliance with this regulation by July 2014 with re-enrollment of all providers completed by March 2016.**

4.46 Provider Screening and Enrollment (Page 2 of 3)

42 CFR 455.416	TERMINATION OR DENIAL OF ENROLLMENT __X__Assures that the State Medicaid agency will comply with section 1902(a)(39) of the Act and with the requirements outlined in 42 CFR 455.416 for all terminations or denials of provider enrollment. **The Department is largely compliant with parts (a), (b), (e) and (f)) of this regulation. The Department expects to be compliant with parts (c) and (d) of this regulation by June 2013.**
42 CFR 455.420	REACTIVATION OF PROVIDER ENROLLMENT __X__Assures that any reactivation of a provider will include re-screening and payment of application fees as required by 42 CFR 455.460. **The Department is compliant with these regulations with the exception of the collection of fees.**
42 CFR 455.422	APPEAL RIGHTS __X__Assures that all terminated providers and providers denied enrollment as a result of the requirements of 42 CFR 455.416 will have appeal rights available under procedures established by State law or regulation. **The Department is currently compliant with this regulation.**
42 CFR 455.432	SITE VISITS __X__Assures that pre-enrollment and post-enrollment site visits of providers who are in “moderate” or “high” risk categories will occur. **The Department is largely compliant with part (a) of these regulations. The Department expects to be compliant with part (b) of these regulations by June 2013.**
42 CFR 455.434	CRIMINAL BACKGROUND CHECKS __X__Assures that providers, as a condition of enrollment, will be required to consent to criminal background checks including fingerprints, if required to do so under State law, or by the level of screening based on risk of fraud, waste or abuse for that category of provider. **The Department expects to be compliant these regulations by June 2013.**

STATE PLAN UNDER TITLE XIX OF THE SOCIAL SECURITY ACT

State/Territory: Colorado

4.46 Provider Screening and Enrollment (Page 3 of 3)

42 CFR 455.436	FEDERAL DATABASE CHECKS __X__Assures that the State Medicaid agency will perform Federal database checks on all providers or any person with an ownership or controlling interest or who is an agent or managing employee of the provider. **The Department expects to be compliant with parts (a), (b) and (c)(1) regulations by June 2013. The Department will begin compliance with part (c)(2) of these regulations by July 2014.**
42 CFR 455.440	NATIONAL PROVIDER IDENTIFIER __X__Assures that the State Medicaid agency requires the National Provider Identifier of any ordering or referring physician or other professional to be specified on any claim for payment that is based on an order or referral of the physician or other professional. **The Department will be partially compliant for non-pharmacy claims in June 2013**. The Department will begin enrollment of prescribing only providers in July 2014. The Department **expects to be fully compliant with these regulations by July 2016.**
42 CFR 455.450	SCREENING LEVELS FOR MEDICAID PROVIDERS __X__Assures that the State Medicaid agency complies 1902(a)(77) and 1902(kk) of the Act and with the requirements outlined in 42 CFR 455.450 for screening levels based upon the categorical risk level determined for a provider. **The Department is largely compliant with these regulations.**
42 CFR 455.460	APPLICATION FEE __X__Assures that the State Medicaid agency complies with the requirements for collection of the application fee set forth in section 1866(j)(2)(C) of the Act and 42 CFR 455.460. **The Department expects to begin compliance with this regulation by July 2014.**
42 CFR 455.470	TEMPORARY MORATORIUM ON ENROLLMENT OF NEW PROVIDERS OR SUPPLIERS __X__Assures that the State Medicaid agency complies with any temporary moratorium on the enrollment of new providers or provider types imposed by the Secretary under section 1866(j)(7) and 1902(kk)(4) of the Act, subject to any determination by the State and written notice to the Secretary that such a temporary moratorium would not adversely impact beneficiaries' access to medical assistance. **The Department is compliant with these regulations.**

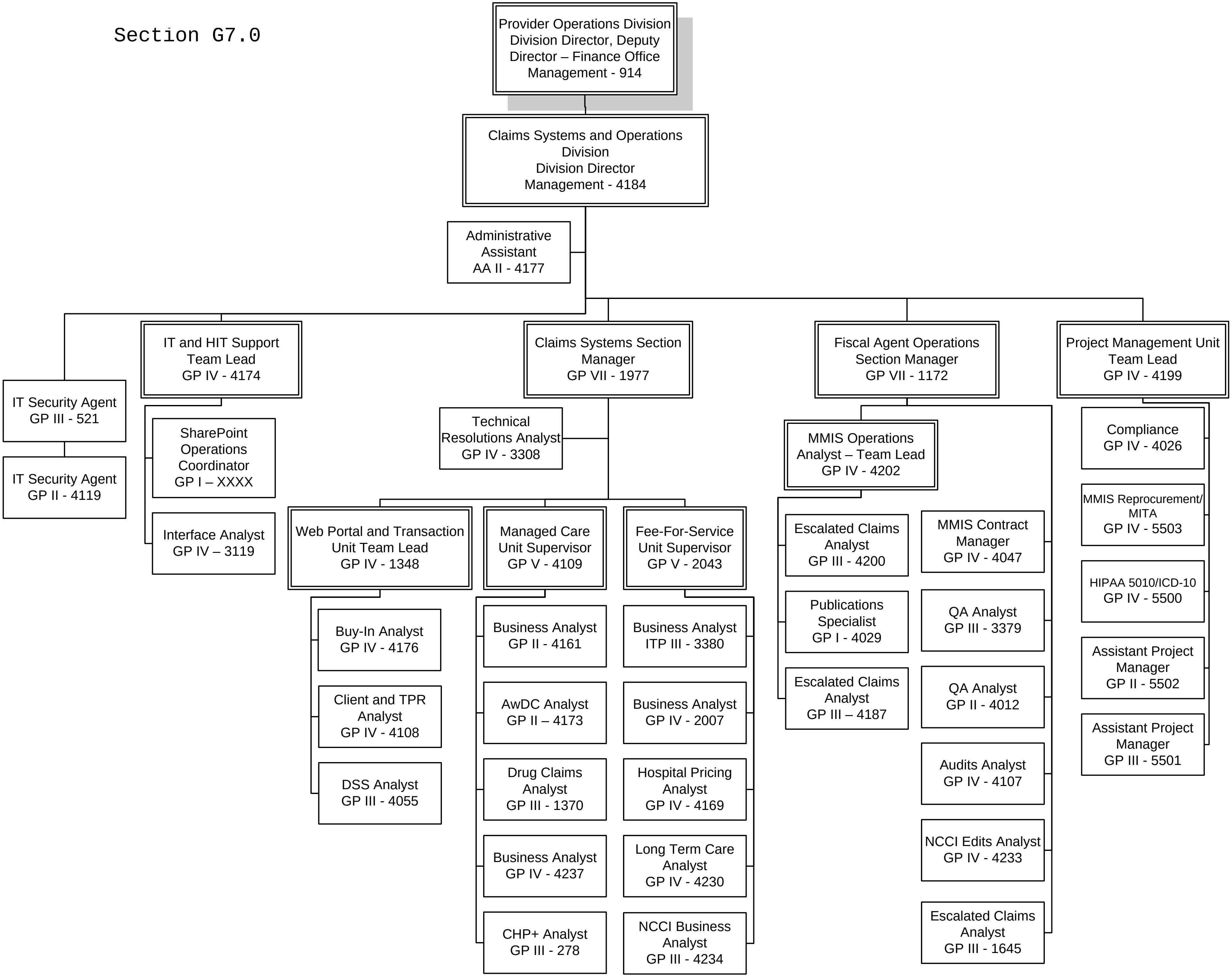
TN **12-009**

APPROVAL DATE: ________________

SUPERSEDES: **New**

EFFECTIVE DATE: **April 1, 2012**

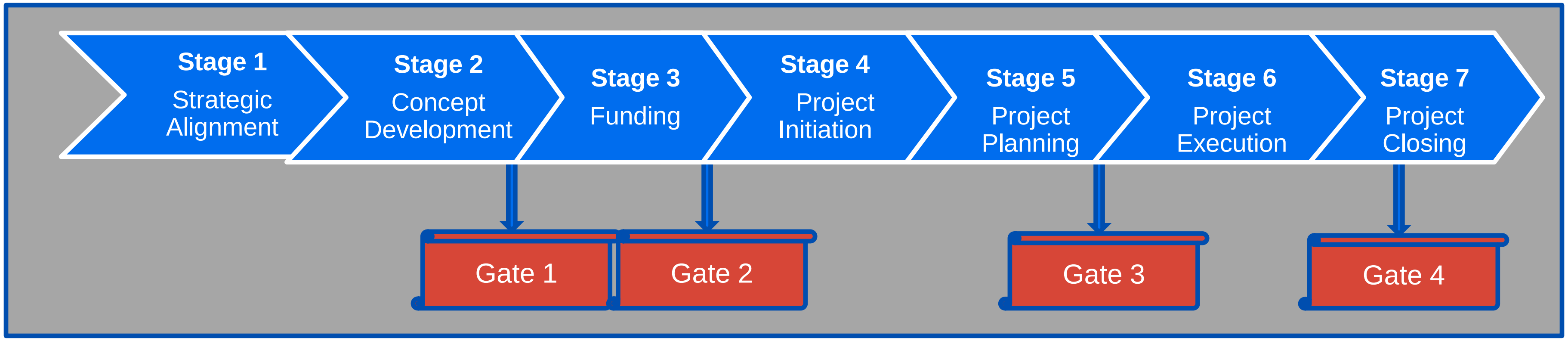
Section G7.0



- Provider Operations Division
Division Director, Deputy Director – Finance Office
Management - 914
  - Claims Systems and Operations Division
Division Director
Management - 4184
    - Administrative Assistant
AA II - 4177
    - IT Security Agent
GP III - 521
      - IT Security Agent
GP II - 4119
    - IT and HIT Support Team Lead
GP IV - 4174
      - SharePoint Operations Coordinator
GP I – XXXX
      - Interface Analyst
GP IV – 3119
    - Claims Systems Section Manager
GP VII - 1977
      - Technical Resolutions Analyst
GP IV - 3308
      - Web Portal and Transaction Unit Team Lead
GP IV - 1348
        - Buy-In Analyst
GP IV - 4176
        - Client and TPR Analyst
GP IV - 4108
        - DSS Analyst
GP III - 4055
      - Managed Care Unit Supervisor
GP V - 4109
        - Business Analyst
GP II - 4161
        - AwDC Analyst
GP II – 4173
        - Drug Claims Analyst
GP III - 1370
        - Business Analyst
GP IV - 4237
        - CHP+ Analyst
GP III - 278
      - Fee-For-Service Unit Supervisor
GP V - 2043
        - Business Analyst
ITP III - 3380
        - Business Analyst
GP IV - 2007
        - Hospital Pricing Analyst
GP IV - 4169
        - Long Term Care Analyst
GP IV - 4230
        - NCCI Business Analyst
GP III - 4234
    - Fiscal Agent Operations Section Manager
GP VII - 1172
      - MMIS Operations Analyst – Team Lead
GP IV - 4202
        - Escalated Claims Analyst
GP III - 4200
        - Publications Specialist
GP I - 4029
        - Escalated Claims Analyst
GP III – 4187
      - MMIS Contract Manager
GP IV - 4047
      - QA Analyst
GP III - 3379
      - QA Analyst
GP II - 4012
      - Audits Analyst
GP IV - 4107
      - NCCI Edits Analyst
GP IV - 4233
      - Escalated Claims Analyst
GP III - 1645
    - Project Management Unit Team Lead
GP IV - 4199
      - Compliance
GP IV - 4026
      - MMIS Reprocurement/ MITA
GP IV - 5503
      - HIPAA 5010/ICD-10
GP IV - 5500
      - Assistant Project Manager
GP II - 5502
      - Assistant Project Manager
GP III - 5501

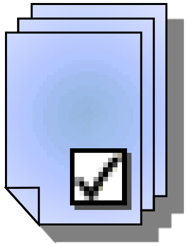
Section G8.0

Governance Process within Project Lifecycle



Phase gate movement:

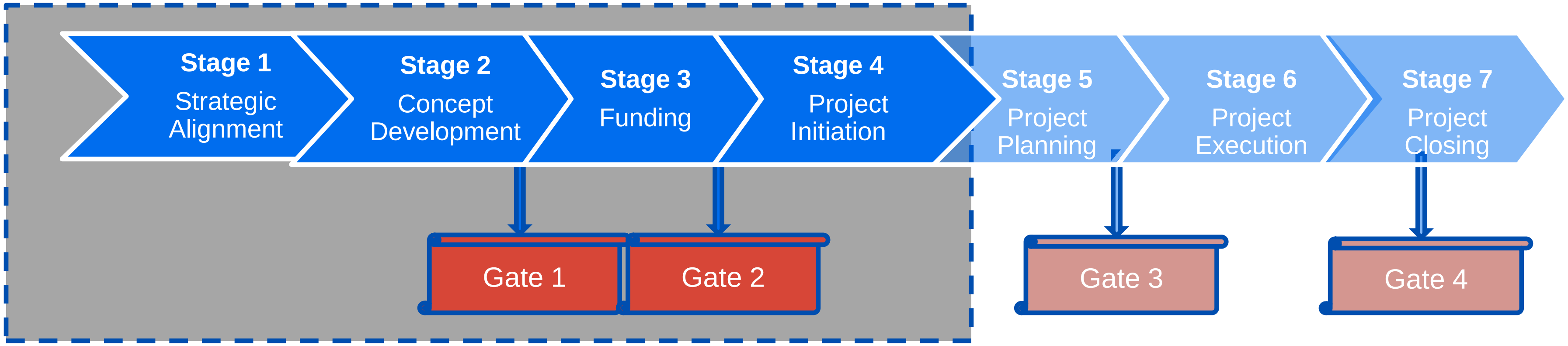
- Defined entrance/exit criteria
- Options for preliminary Agency review
- “Pre-approval” process for requesting Governance review
  - Board administrator
  - Potential workflow management

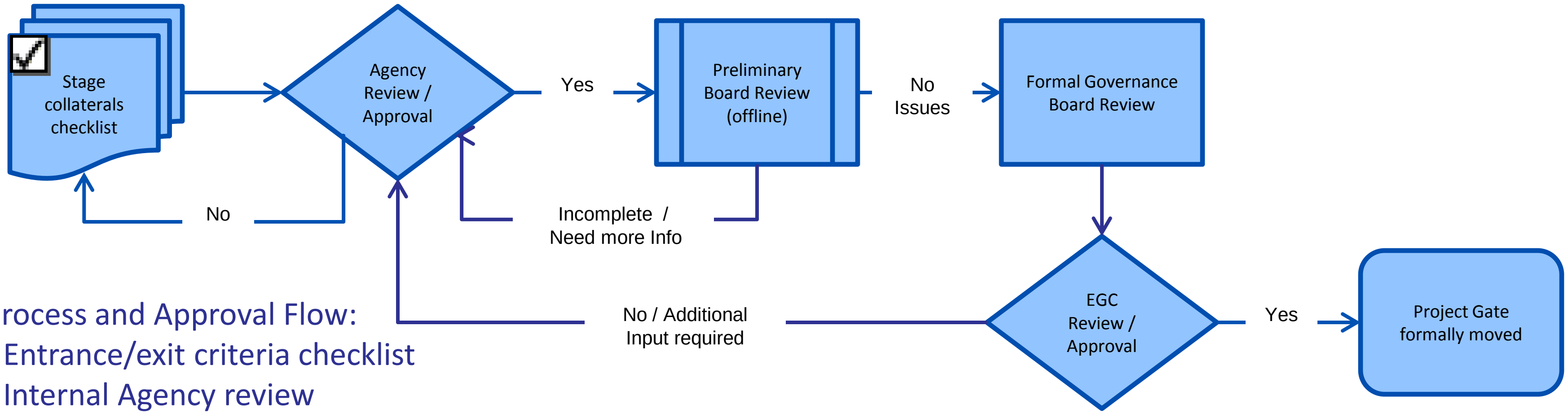


Governance approval options:

- Formal board meeting and review
- Electronic management of collateral and approvals
- Future workflow automation

Project Initiation Governance Flow




Stage collaterals checklist
Agency Review / Approval
Yes
No
Preliminary Board Review (offline)
No Issues
Incomplete / Need more Info
Formal Governance Board Review
EGC Review / Approval
No / Additional Input required
Yes
Project Gate formally moved

Process and Approval Flow:

- Entrance/exit criteria checklist
- Internal Agency review
- Preliminary Governance review
  - Pre-approval (collateral review)
  - Formal board review
- Gate move approved

Section G9.0

MMIS TURNOVER PLAN

FOR

TRANSFER OF

MMIS SYSTEM AND OPERATIONS
12 Month Update

June 30, 2009

Introduction

The requirements for this document are defined in Article, 4 Tasks 4.7-4.7.3 of the Request for Proposals for the Replacement and Enhancement of a Medicaid Management Information System. A copy of Article 4 is located in Appendix #1.

MMIS Turnover Project

The objective of the MMIS Turnover Task is to provide for an orderly, complete, and controlled transition to a successor contractor, and to minimize any disruption of processing and services provided to Colorado Medical Assistance Program recipients, providers, and operational users of the system. The following topics are discussed regarding ACS's MMIS turnover management approach:

- Proposed approach to turnover
- Phases, tasks, and subtasks for turnover
- Schedule for turnover
- Production program and documentation update procedures during turnover

1. Proposed Approach to Turnover

It is ACS's responsibility to maintain stable operations of the Colorado MMIS while turnover activities proceed. To this end, ACS updates and follows a detailed turnover plan that coordinates regular account functions while providing the necessary support to ensure a smooth Colorado MMIS turnover.

As part of the Turnover plan, ACS will designate a Turnover Coordinator to act as the liaison between the Department, and ACS. This person will serve part time until the department initiates a request for turnover activities, at that point the Turnover Coordinator will work full time until termination of the contract.

Sherri Gouthier will serve as the Turnover Coordinator for ACS and will coordinate and monitors all turnover activities. The ACS senior management team or Sherri can be contacted in relation to turnover activities.

Once ACS receives notice from the Department to transfer the MMIS, ACS conducts the turnover of files and turnover training by separating the Colorado MMIS functions, first by subsystem and then by manual and system procedures within each subsystem. An automated project tracking mechanism is used to ensure that all deliverable requirements are met.

ACS develops electronic and hard copy document deliverable schedules based upon the final cycle execution update or content modification of each file. The dates reflect the latest times that files may be expected to arrive at the transferring entity's data center, and are based upon estimates of cycle production times, copying files, and shipment to the off-site entity.

Assumptions and Constraints

This Turnover Plan is based on several assumptions regarding scheduling, and has established certain constraints to allow current operations to proceed. The Department should review these assumptions and constraints carefully to ensure minimal impact of the turnover on the provider and client communities.

- Final schedules for all cycle processes are determined and published as part of the updated Turnover Plan document, due six (6) months prior to the final system transfer.
- The turnover ending date is based upon a relative turnover date. The Department should notify ACS of any extensions six (6) months prior to the end of the current contract.
- Updating of reference, provider, and rates files ceases at an agreed upon amount of time prior to the turnover date to allow completion of all ongoing activities and finalization of in process claims and update transaction processes.
- Ten (10) working days are required to allow for the completion of the final processing cycles and transfer of the remaining data files.

- No new claims, either electronic or hard copies, are accepted during the final five (5) working days prior to the transfer date, with the exception of point-of-sale drug claims. This allows the complete resolution of all edits and adjudication of claims to be transferred.

ACS establishes the final system file turnover dates based upon the final cycle execution or update of each file. Final file and data transfer schedules include the expected delivery times of the electronic media or documents included in the transfer process.

Statement of Resource Requirements

At least twelve (12) months prior to the start of the last year of the base contract period, the contractor shall furnish, at no extra charge, a statement of the resources that would be required by the Department or another contractor to fully take over Fiscal Agent functions of the MMIS.

The statement must include an estimate of the number, type, and salary of personnel required to perform the other functions of the Colorado MMIS. The statement shall be separated by type of activity of the personnel, including, but not limited to, the following categories:

1. Data processing staff (for modification support)
2. Systems analysts
3. Systems programmers
4. Programmer analysts
5. Administrative staff
6. Clerks
7. Managers
8. Medical personnel (nurses, MDs, pharmacists, etc.)
9. Other support staff (TPL, SURS, Provider/Client Relations)

The statement shall include all facilities and any other resources required to operate the Colorado MMIS, including, but not limited to:

1. Telecommunications networks
2. Office space
3. Hardware
4. Software
5. Other

The statement of resource requirements shall be based on the contractor's experience in the operation of the MMIS and shall include actual contractor resources devoted to Fiscal Agent operations.

With respect to office (physical) facilities, ACS currently uses 25,372 square feet of office space to perform its current Colorado Fiscal Agent MMIS Operations. This does not include offsite support space.

2. Phases, Tasks and Subtasks for Turnover

An automated project tracking mechanism (such as Microsoft Project) is used to ensure that all deliverable requirements are identified, and progress towards the goals is tracked against the project completion dates. The turnover plan is intended to clearly define tasks and subtasks which must be completed prior to turnover of the Colorado MMIS. Within each task, subtasks define the activities that must be completed prior to turnover of the Colorado MMIS.

The high-order tasks are as follows:

1. Notify ACS of intent to initiate the transfer of the MMIS

2. Complete Turnover Plan

3. Deliver Plan and request review and approval of Turnover Plan from DHCPF

4. State approval of the MMIS Turnover Plan is provided

5. Complete Development of the MMIS Requirements Statement, including:

    5.1. Staff
        5.1.1. Data Processing Staff (for modification support)
        5.1.2. Systems Analysts
        5.1.3. Systems Programmers
        5.1.4. Programmer Analysts
        5.1.5. Administrative staff
        5.1.6. Managers
        5.1.7. Medical personnel (nurses, MDs, pharmacists, etc)
        5.1.8. Other support staff
            5.1.8.1. TPL
            5.1.8.2. SURS
            5.1.8.3. Provider/Client relations
    5.2. Telecommunications networks
    5.3. Hardware
    5.4. Software
    5.5. Office space

6. Establish a Turnover date and final schedules

7. Update Turnover Plan

8. Update Turnover Requirements Statement

9. Develop Training Plan Containing sessions for:
    9.1. Claims processing data/exam entry
    9.2. Exemption claims processing

9.3. Other manual procedures

10. Conduct training for State staff or the designated fiscal agent in the operation of the MMIS
    10.1. Claims processing data/exam entry
    10.2. Exemption claims processing
    10.3. Other manual procedures

11. Execute final Colorado MMIS cycles and Transfer Colorado MMIS electronic and hard copy data files

12. Remove Hardware from State Offices

13. Transfer State-owned Hardware to State Offices

3. Schedule for turnover

Anticipated Turnover Project Schedule

The anticipated start date of the Colorado MMIS Turnover Project is dependent upon the agreed upon date on which the contract is to be terminated. Prior to the beginning of the turnover activities, the MMIS Turnover Plan must be formally approved by DHCPF.

Prior to the start of the last year of the agreement, ACS prepares updates and delivers a Requirements Statement document listing the resources that would be required by the State or another contractor to take over operation of the MMIS and the claims submission software. Over time, the resources of an operational Fiscal Agent account change as a result of changes in workload, staffing efficiencies and system modifications. These changes are reflected in all iterations of the Turnover Plan and the Requirements Statement.

At the six (6) month interval before transition, the current staffing and system components required for operation of the Colorado MMIS are identified in the inventory list of the Requirements Statement document provided to the Department.

This Turnover Plan document is updated again six (6) months prior to the transfer of processing responsibility. The Turnover Plan is reviewed by the turnover support team to ensure that it identifies all tasks necessary to transfer the Colorado MMIS to the Department or another fiscal agent. The turnover team identifies all areas of systems and operation in which transfer of the current MMIS is needed. The schedule is refined to comprehensively identify turnover dates, activities and deliverables. The plan includes a complete list of production programs and data files required by the receiving contractor or the State to operate the system.

The schedules identify the following events for each of the MMIS subsystem processing components:

- Final Cycle Execution Date
- System File Transfer Date
- Manual Activities Completion Date
- Manual File Transfer Date

Actual completion dates will be mutually determined and agreed upon by DHCPF and ACS, and based upon existing inventories and ACS's production capabilities during the final months of the contract.

At the time the turnover date is established, ACS notifies the Department of the final dates for receipt of input data for MMIS final cycle execution, as well as the dates at which on-line files can be used for inquiry-only purposes. ACS and DHCPF mutually agree upon the schedule.

The Turnover Plan also includes a process to provide DHCPF with all program and documentation updates on any modifications that are made to the system during the turnover period. The turnover support team develops a deliverable receipt form and identifies a method of tracking all deliverables to the Department.

Five (5) months prior to the end of the contract, ACS prepares a training plan and begins training the staff of the State or its designated agent in the operation of the MMIS. Such training is to be concluded at least three (3) months prior to the end of the contract in accordance with Colorado RFP requirement 4.7.1.3

The plan contains the following information:

- Schedules of training sessions
- Training locations
- Names of instructors and training assistants
- Needed supplies
- Equipment requirements
- Training methods
- Subject matter
- Class sizes
- Planned training materials

ACS prepares training materials to reinforce the topics covered in the classes, and provides reference materials that the trainees can use later in their jobs. Wherever possible, existing user manual documentation is used during the training to assist State staff or the designated agents. Training materials typically include documentation, flow charts, and if appropriate, screen-prints from the Colorado MMIS. Online training is used to guide trainees through a variety of MMIS functions. Each functional component includes descriptions of the automated and manual components or processes required to perform the identified job activity.

Training is completed at least three (3) months prior to the end of the turnover task. Such training includes sessions for:

- Claims processing data/exam entry
- Exception claims processing
- Other manual procedures

Turnover Project Deliverables

The defined deliverables for the turnover project include:

- Turnover Plan
- Requirements Statement
- Software, files, and operations and user documentation

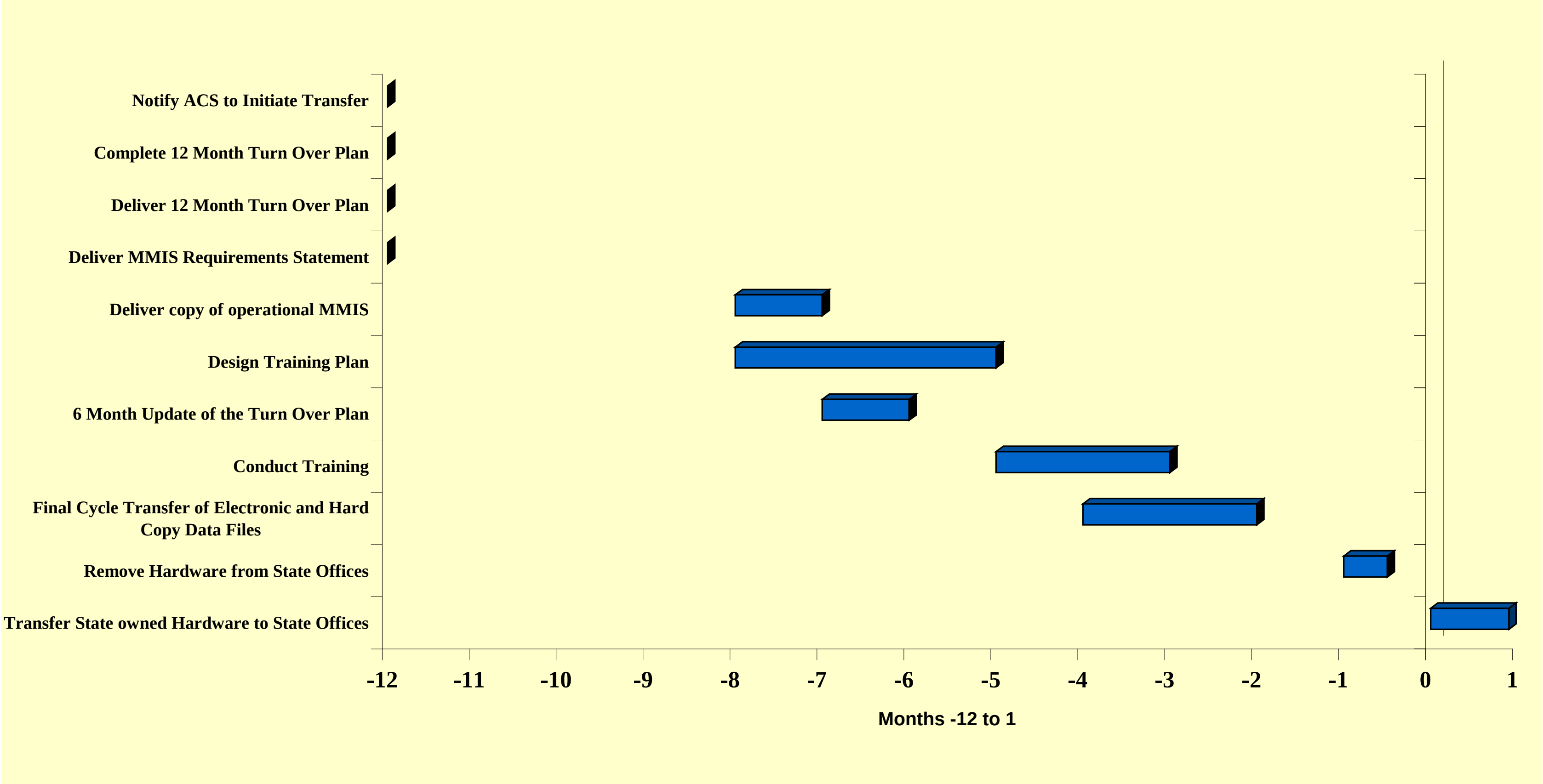
The Turnover Plan and the Requirements Statement are revised, delivered, and approved by the Department at specified intervals as described earlier in this document. Attached to each deliverable is a receipt form describing the item and requesting either an approval or a return with comments. The Department must formally approve all deliverables before successor tasks may be initiated.

Turnover Project Time Line

The chart on the following page identifies the high order tasks in the turnover project and the relative months of delivery or performance based on a twelve (12) month time line, including all updates for the turnover/transfer of the Colorado MMIS. As referred to above, the turnover ending date is based upon a relative turnover date as determined and agreed upon by the Department and ACS, at least six (6) months prior to the end of the contract period.

The twelve (12) month update of Turnover Project Timeline is the time period required for an orderly transfer of the MMIS and Fiscal Agent Operations. Although the delivery for items identified herein may be accelerated, it is believed that accelerating any deliverable time lines in the final six (6) months prior to transfer would adversely impact the overall success of the MMIS transfer.

Turnover Task Time Scale



4. Production program and documentation update procedures during turnover

ACS continues to be responsible for providing to the Department complete, accurate, and timely documentation of the MMIS. During the turnover project, ACS continues to provide consultation to the State in the development of maintenance and modification requests. All major changes and modifications resulting from CSRs are based upon requirements statements and processing plans, and all procedures and standards relating to software development, documentation, system testing and implementation are followed.

ACS continues to prepare updates to the MMIS Systems Documentation, incorporating all changes, corrections, or enhancements to the MMIS. Updates to the MMIS Systems Documentation are delivered to the State within ten (10) business days of Department approval of implementation of the change, unless otherwise agreed to by DHCPF.

During the final six (6) months of the contract, the number and scope of enhancements to the system are significantly reduced to allow for the orderly and controlled transfer of processing responsibilities. Only those CSRs and system changes that can be finalized and fully implemented prior to the transfer and acceptance testing of the transferred system are allowed to proceed. Other system and process modification work is curtailed during this period.

Appendix 1
Article 4 Tasks 4.7-4.7.3
Colorado MMIS RFP

4.7.TURNOVER

Prior to the conclusion of the contract, the Fiscal Agent contractor shall provide, at no extra charge, assistance in turning over the final contractor responsibilities to the Department or its agent.

4.7.1. Contractor Responsibilities

4.7.1.1. Develop an MMIS Turnover Plan

At least twelve (12) months before the start of the first option year of the contract, the contractor shall provide, at no additional cost, a Turnover Plan to the Department. The plan shall include:

1. Proposed approach to turnover
2. Tasks and subtasks for turnover
3. Schedule for turnover
4. Documentation update procedures during turnover

4.7.1.2. Develop an MMIS Requirements Statement

At least twelve (12) months prior to the start of the last year of the base contract period, the contractor shall furnish, at no extra charge, a statement of the resources that would be required by the Department or another contractor to fully take over Fiscal Agent functions of the MMIS.

The statement must include an estimate of the number, type, and salary of personnel required to perform the other functions of the Colorado MMIS. The statement shall be separated by type of activity of the personnel, including, but not limited to, the following categories:

10. Data processing staff (for modification support)
11. Systems analysts
12. Systems programmers
13. Programmer analysts
14. Administrative staff
15. Clerks
16. Managers
17. Medical personnel (nurses, MDs, pharmacists, etc.)
18. Other support staff (TPL, SURS, Provider/Client Relations)

The statement shall include all facilities and any other resources required to operate the Colorado MMIS, including, but not limited to:

6. Telecommunications networks
7. Office space
8. Hardware
9. Software
10. Other

The statement of resource requirements shall be based on the contractor's experience in the operation of the MMIS and shall include actual contractor resources devoted to Fiscal Agent operations activities.

4.7.1.3. Provide Turnover Service

As requested, but approximately six (6) months prior to the end of the base contract period or any extension thereof, transfer to the Department or its agent, as needed, a copy of the operational MMIS on media determined by the Department, including:

Documentation, including, but not limited to, user, provider, and other manuals needed to maintain the system.

As requested, but approximately five (5) months prior to the end of the contract or any extension thereof, begin training Department staff, or its designated agent, in the Fiscal Agent operations activities of the MMIS. Such training must be completed at least three (3) months prior to the end of the contract or any extension thereof. Such training shall include:

1. Claims processing data/exam entry
2. Exception claims processing
3. Other manual procedures

4.7.1.4. Update MMIS Turnover Plan

At least six (6) months prior to the end of the base contract and at least six (6) months prior to the end of any contract extension, the contractor shall provide an updated MMIS Turnover Plan and MMIS Requirements Statement.

4.7.2. Department Responsibilities

1. Review and approve a Turnover Plan to facilitate transfer of the Fiscal Agent responsibilities to the Department or its designated agent.
2. Review and approve a statement of staffing and non-mainframe resources that would be required to take over operation.
3. Request turnover services are initiated by the contractor.
4. Make Department staff or designated replacement Fiscal Agent staff available to be trained in the operation of the MMIS.

4.7.3. Turnover Staffing Requirements

Beginning with the submission of the initial Turnover Plan and Resource Statement, the contractor shall designate a staff person as Turnover Coordinator. This individual shall have a Systems Analysis background and shall serve part-time in this capacity until the Department initiates a request for turnover activity. At the time that the Department requests that the contractor initiate turnover activity, this individual shall become a full-time Turnover Coordinator until termination of the contract.

4.

MMIS TURNOVER PLAN

REQUIREMENTS STATEMENT

FOR

TRANSFER OF

MMIS SYSTEM AND OPERATIONS
12 Month Update

June 30, 2009

Section #1
ACS Colorado MMIS Statement of Resource Requirements

Introduction

This is the 12 month update to the MMIS Turnover Plan Requirements Statement. The requirements for this document are defined in Article 4, Task 4.7.1.2 of the "Request for Proposals for MMIS Takeover and Fiscal Agent Services." A copy of this article is located in Section #5.

Statement of Resource Requirements

The following identifies the updated resources currently used by ACS in its administration of the Colorado MMIS and its operations in accordance with the RFP requirements.

- The ACS Colorado MMIS Staffing Matrix in Section #2 meets RFP requirement 4.7.1.2 which states the Contractor shall include an estimate of the number and type of personnel required to operate the equipment and perform the other functions of the MMIS. This Staffing Matrix is comprised of 100 Full Time Equivalent (FTE) employees. The breakdown of these employees is:
  - 54 Exempt Employees
  - 46 Non-Exempt Employees
- As required by RFP requirement 4.7.1.2, the statements of resource requirements contained in this document are based on ACS' experience in the operation of the MMIS, and reflect actual Contractor resources devoted to the operation of the system. These statements are contained in Section #3 – PC and Server Configurations and Section #4 – Colorado MMIS RFP Inventory Recap. These two sections identify the resources required by ACS to operate the MMIS, including, at a minimum, data processing hardware/equipment, system and special software, other equipment, telecommunications circuits, and any other requirements.

With respect to office (physical) facilities, ACS currently uses 25,372 square feet of office space to perform its current Colorado Fiscal Agent MMIS Operations. This does not include offsite support space.

Section #2
ACS Colorado MMIS Staffing Matrix

Department	# of FTE's
Account Manager	1
Business Ops Manager	1
Business Services	5
Claims Operations	20
Claims Processing Manager	1
Deputy Account Manager	1
Financial Analyst	1
LAN Manager	1
Medical Policy Manager	1
Medical Review	5
Operations Supervisor	2
Professional Services	11
Professional Services Manager	1
Provider Relations Manager	1
Provider Services	19
Quality Control	4
State Trainer	1
Systems	22
Systems Manager	1
Systems QA	1

Section #3
PC and Server Configurations

Basic PC configuration

Workstation Software Configuration		
Type	**OS**	**Software**
Basic	MS XP Pro.	McAfee, Adobe Reader, Office 2003, Compatibility Pack for Office 2007, MMIS, COLD, Ad-aware SE, Microsoft Visual C++ 2005 Redistributable Package
Call Center	MS XP Pro.	McAfee, Adobe Reader, Office 2003, Compatibility Pack for Office 2007, MMIS, COLD, Avaya Agent/Wallboard, Omnitrack, DocFinity, Ad-aware SE, Spark, Microsoft Visual C++ 2005 Redistributable Package
Systems BA/PA	MS XP Pro.	McAfee, Adobe, Office 2003, Compatibility Pack for Office 2007, MMIS, COLD, Trackwise, RUMBA, Business Objects, Visio Viewer, Ad-aware SE, CutePDF Writer, Microsoft Visual C++ 2005 Redistributable Package

Other Software (as needed)

Misc. Software
TN3270
Avaya CMS Supervisor
FaxPress
MS Project 2000
MS Publisher 2000
MS Visio 2003
UltraEdit

Server Configurations

Server Software Configuration		
Server Name	**OS**	**Applications**
ACSDENVER-CCE	Windows 2003 Server	Avaya Contact Center Express
ACSDENVER-SQL	Windows 2003 Server	MS SQL 2005
ACSIVR	Windows 2000 Server	EPOS Firstline Encore 7.3 / Xpressboot
AGDEN0SLPDB01	Red Hat Enterprise Linux 5 Server	ESURS Datamart Server
AGDEN0SVPDM01	Vmware ESX 3i	VMWare
AGDEN0SWPDM01	Windows 2003 Enterprise	COGNOS Web Server
AGDEN0SWPDM02	Windows 2003 Server	COGNOS Application Server
AGDEN0SWPDM03	Windows 2003 Server	VMWare Host
AGDEN0SWPDM04	Windows 2003 Server	
AGDEN0SWPDM05	Windows 2003 Server	ESURS Application Server
AGDEN0SWPFP01	Windows 2003 Server	Part of server migration project of combining DENPDC01 and DENBDC01 stand alone servers in to rack configuration
AGDEN0SWPSM01	Windows 2003 Server	Dell Desktop Manager
AGDEN0SWPSM02	Windows 2000 Server	Symantec Ghost Console 2.1
AGDEN0SWTFP01	Windows 2003 Server	Wildfire 3.2.0 IM Server / Spiceworks Asset Management
AGDEN0SWTFP02	Windows 2003 Server	VMWare
AGDEN0SWVPDM01	Windows 2000 Server	
AGDEN0SWVPS	Windows 2003 Server	Voice Print 2.83 / Firebird SQL Database 1.5.3
AGDENSWRBK01	Windows 2003 Server	Symantec Ghost Console 2.1
CO-APPS1	Windows 2000 Server	Business Objects
CO-APPS2	Windows 2000 Server	Business Objects
CO-ETL	Windows 2000 Server	DSS File Server
COPROD	Solaris 9	DSS Database Server

DELL0093N	Windows 2000 Server	McAfee EPO
DELL0147	Windows 2003 Server	Denver Helpdesk Ticketing System
DENBDC01	Windows 2003 Server	MMIS_PROD / MMIS_Unit_Test / Trackwise / MS SQL Server / Consultrack
DENOITAPPSVR	Windows 2003 Server	Netbackup 5.1 / Docfinity Object Importer
DENOITSQLSVR	Windows 2003 Server	MS SQL
DENOITWEBSVR	Windows 2003 Server	Cold Fusion 6.0
DENOTRACK1	Windows 2000 Server	Sybase SQL Central 4.1.1.1370
DENPDC01	Windows 2003 Server	MMIS _Test / MMIS_System/ Script Logic
DENPRTSVR01	Windows 2003 Server	WSUS 3.0
DENTERM01	Windows 2000 Server	Citric MetaFrame XP Feature Release 2 / Terminal Services Windows 2000 Server

Section #4
Colorado MMIS RFP Inventory Recap

DENVER Resources

Hardware Inventory					
Vendor	**Quantity**	**Model #**	**CPU**	**# Drives / Drive Capacity**	**Memory**
Servers					
DELL	1	PowerEdge 1600SC	Dual Xeon / 2.0GHz	2/36 GB	512 MB
DELL	1	PowerEdge 2400	PIII / 733MHz	4/9.2 GB	4 GB
DELL	1	PowerEdge 2500	PIII / 1.0GHz	3/'36 GB	2 GB
DELL	1	PowerEdge 2600	Dual Xeon / 2.4GHz	4/73 GB	2 GB
DELL	1	PowerEdge 2850	Xeon / 3.0GHz	6/36 GB	2 GB
DELL	1	PowerEdge 2850	Dual Xeon / 3.0GHz	6/73 GB	2 GB
DELL	1	PowerEdge 2850	Xeon / 3.0GHz	6/73 GB	2 GB
DELL	1	PowerEdge 2950	Dual Dual-Core Xeon / 2.0GHz	3/278.88GB	4 GB
DELL	1	PowerEdge 2900	Dual-Core Xeon / 1.86GHz	2/146 GB	1 GB
DELL	1	PowerEdge 2950	Dual Quad-Core Xeon / 2.0 GHz (E5405)	3/300 GB	4 GB
DELL	1	PowerEdge 2950	Dual Quad-Core Xeon / 3.0GHz (E5450)	2/750GB	32 GB
DELL	5	PowerEdge 2950	Dual Quad-Core Xeon / 2.0GHz (E5335)	3/300 GB	4 GB
DELL	1	PowerEdge 4400	PIII / 1.0GHz	4/9.2 GB / 4/73 GB	1 GB
DELL	2	PowerEdge 4600	P4 / 2.4GHz	8/36 GB	4 GB
DELL	2	PowerEdge 860	Dual-Core Xeon / 2.4GHz	1/80 GB	2 GB
DELL	1	PowerEdge R900	Quad Dual-Core Xeon / 2.93GHz	5/300GB	64 GB
HP/COMPAQ	1	Proliant DL360R03	Dual Xeon / 2.4GHz	2/36.4 GB	4 GB
HP/COMPAQ	2	Proliant DL380R03	Quad Xeon / 2.8GHz	4/36.4 Gig	4 GB
HP/COMPAQ	1	Proliant DL380R03	Quad Xeon / 1.9GHz	4/72.8 GB	12 GB
HP/COMPAQ	1	Proliant DL580R02	Quad Xeon / 1.9GHz	4/ 72.8 GB	4 GB
SUN	1	SunFire V880	Quad Sun UltraSPARCIII / 900MHz	6/73 GB	16 GB
Total	28				
Workstations					
IBM	5	8215D1U	Intel Pentium 43000 MHz	80 GB	1 GB
IBM	36	8215D1U	Intel Pentium 43000 MHz	80 GB	512 MB
DELL	1	Inspiron 2500	Intel Celeron800 MHz	10 GB	128 MB
DELL	1	Inspiron 2600	Intel Celeron1200 MHz	20 GB	640 MB
DELL	1	Latitude C640	Mobile Intel Pentium 4 - M2000 MHz	20 GB	512 MB
DELL	2	Latitude D630	Intel(R) Core(TM)2 Duo2000 MHz	80 GB	1 GB
DELL	2	Latitude D830	Intel(R) Core(TM)2 Duo2000 MHz	120 GB	2 GB
DELL	1	Latitude E6400	Intel(R) Core(TM)2 Duo2400 MHz	80 GB	2 GB
DELL	23	OptiPlex 330	Intel(R) Pentium(R) Dual1600 MHz	80 GB	1 GB
DELL	29	OptiPlex 330	Intel(R) Pentium(R) Dual2000 MHz	80 GB	2 GB
DELL	7	OptiPlex 360	Intel(R) Core(TM)2 Duo2200 MHz	80 GB	2 GB
DELL	5	OptiPlex 755	Intel(R) Core(TM)2 Duo2200 MHz	80 GB	4 GB
DELL	1	OptiPlex GX260	Intel Pentium 42700 MHz	20 GB	1 GB
DELL	1	OptiPlex GX260	Intel Pentium 42700 MHz	40 GB	512 MB
DELL	5	OptiPlex GX260	Intel Pentium 42700 MHz	20 GB	512 MB

DELL	1	OptiPlex GX260	Intel Pentium 42700 MHz	20 GB	640 MB
DELL	1	OptiPlex GX260	Intel Pentium 42800 MHz	40 GB	1 GB
DELL	2	OptiPlex GX260	Intel Pentium 42800 MHz	40 GB	384 MB
DELL	3	OptiPlex GX260	Intel Pentium 42800 MHz	20 GB	384 MB
DELL	2	OptiPlex GX260	Intel Pentium 42800 MHz	20 GB	512 MB
DELL	1	OptiPlex GX260	Intel Pentium 42800 MHz	20 GB	768 MB
DELL	1	OptiPlex GX270	Intel Pentium 42800 MHz	40 GB	512 MB
DELL	1	Precision WorkStation T3400	Intel(R) Core(TM)2 Duo2000 MHz	150 GB	3 GB
Total	132				
Printers					
HP	1	Color LaserJet 4600DN			
HP	1	LaserJet 4100DTN			
HP	1	LaserJet 4100N			
HP	1	LaserJet 5SiMX			
HP	1	LaserJet 8150DN			
HP	1	LaserJet 9000			
Lanier	1	LD151 MFD			
Total	**7**				
Scanners					
Kodak	1	Kodak i810			

Communication Resources:

Networking Devices	
Model	**Quantity**
Cisco Catalyst 4510R Switch	1
Cisco PIX 515 Firewall	2
Cisco 2821 Router	2
Cisco 1841 Router	1
Total	**6**

PBX - Voice Hardware	
Model	**Quantity**
Avaya S8500 Media Server	1
Avaya Audix	1
Avaya Call Master IV phones	27
Avaya 6408D+ phones	70
Avaya 8405B+ phones	29
Total	**128**

Network Circuits	
Model	**Quantity**
MPLS T1 - ACS Network	4
PTP T1 - State Network	1
PTP T1 - HSAG Netwokr	1
PTP T1 - Maximus Network	1
Total	**7**

Voice Circuits	
Model	**Quantity**
AT&T Long Distance	2
Quest Local	2
POTS Line	2
Total	**6**

End of Denver Resources --

Section #5
Article 4 Task 4.7.1.2
Colorado MMIS RFP

4.4.1.1. Develop an MMIS Requirements Statement

At least twelve (12) months prior to the start of the last year of the base contract period, the contractor shall furnish, at no extra charge, a statement of the resources that would be required by the Department or another contractor to fully take over Fiscal Agent functions of the MMIS.

The statement must include an estimate of the number, type, and salary of personnel required to perform the other functions of the Colorado MMIS. The statement shall be separated by type of activity of the personnel, including, but not limited to, the following categories:

1. Data processing staff (for modification support)
2. Systems analysts
3. Systems programmers
4. Programmer analysts
5. Administrative staff
6. Clerks
7. Managers
8. Medical personnel (nurses, MDs, pharmacists, etc.)
9. Other support staff (TPL, SURS, Provider/Client Relations)

The statement shall include all facilities and any other resources required to operate the Colorado MMIS, including, but not limited to:

1. Telecommunications networks
2. Office space
3. Hardware
4. Software
5. Other

The statement of resource requirements shall be based on the contractor's experience in the operation of the MMIS and shall include actual contractor resources devoted to Fiscal Agent operations activities.