
90FQ0006
Oklahoma Interoperability Grant Project

Oklahoma Interoperability Grant
Data Roadmap

Revision: 2.0
Date: April 26, 2013



Prepared for:
Office of Grants Management
Administration for Children and Families (ACF)
US Department of Health and Human Services
Washington, DC

Prepared by:
Oklahoma Office of Management and Enterprise Services –
Information Services Division serving the
Oklahoma Department of Human Services (OMES-ISD@OKDHS)
Oklahoma City, Oklahoma

Approval Signatures

Signature on File in Project Files

Sumita Pokharel, Project Team Lead

Signature on File in Project Files

James Conway, Project Sponsor

Signature on File in Project Files

Aleta Seaman, OMES–ISD Director

Document Revision Record

Date	Revision	POC	Summary of Changes
04.26.2013	Rev – 2.0	Sumita Pokharel	Updated with additional information and diagrams
02.20.2013	Rev – 1.0	Sumita Pokharel	Initial release of document.

The current version of this document is stored electronically within the OKDHS Source Control System.

Table of Contents

1	Executive Summary	1
1.1	Purpose	1
1.1.1	Goals/Objectives.....	1
1.1.2	Project Outcomes	1
1.2	Background/Overview	2
1.2.1	Exploration Questions/Answers	2
1.2.2	Options Considered	4
1.2.2.1	Master Data Management for eMPI	4
1.2.2.2	Potential Tools	5
1.2.2.2.1	Potential eMPI Tool	5
1.2.2.2.2	Potential MDM Tools	5
1.2.2.2.3	Potential NIEM Tools.....	5
1.2.2.2.4	Potential Tools for Data Governance.....	6
1.2.3	Options Impact and Goals	8
1.2.3.1	Improve Service Delivery for Clients	8
1.2.3.2	Reduce Errors and Improve Program Integrity.....	9
1.2.3.3	Improve Administrative Efficiency	10
2	Scope	10
2.1	Options Enterprise Architecture and/or Modules	10
2.2	End Result.....	10
2.3	Breadth.....	10
2.4	Human Services Program and Initiatives.....	11
2.5	Information Technology Initiatives	11
2.6	Health Intersection.....	12
2.7	Assumptions and Constraints.....	12
2.8	Benefit to Other States	14
3	Approach	14
3.1	AS-IS Overview	14
3.2	TO-BE System.....	17
3.2.1	National Human Services Interoperability Architecture (NHSIA).....	17
3.2.1.1	NHSIA Information Viewpoint Artifacts.....	18
3.2.2	National Information Exchange Model (NIEM).....	21
3.2.2.1	NIEM Governance.....	22
3.2.2.2	NIEM Human Services (HS) Domain Overview	23
3.2.2.3	NIEM Human Services (HS) Domain Governance Structure	23
3.2.2.4	NIEM-UML	25
3.2.2.4.1	Components of NIEM-UML Specification	27
3.2.3	Medicaid Information Technology Architecture (MITA)	28
3.2.3.1	MITA Framework – Information Architecture (IA)	28
3.2.3.2	Data Management Strategy	29
3.2.3.3	MITA Governance Structure.....	29
3.2.3.4	IA Data Architecture	30

3.2.3.5	Data-Sharing Architecture	31
3.2.3.6	Data Standards	31
3.2.3.7	Data Sharing – Master Data Management (MDM)	33
3.2.4	Master Data Management (MDM)	34
3.2.4.1	IBM’s Reference Architecture (RA)	35
3.2.4.2	Data Offered by the MDM Hub.....	38
3.2.4.3	SOA, MDM, and Middleware.....	38
3.2.4.4	Software AG Process–Driven Master Data Management	39
3.2.5	Case Studies for eMPI	40
3.2.6	System Diagram – Data Flows to/from Business Processes	44
3.2.7	Security and Integrity	46
3.2.8	Recommended Approach	48
4	Data Governance.....	49
4.1	Mission and Vision.....	50
4.2	Goals/Metrics.....	50
4.3	Challenges of Data Governance.....	51
4.4	Organization Levels and Roles for Implementing Data Governance	52
4.5	Components of Data Governance	55
4.6	Data Governance Maturity Models	56
4.6.1	Gartner EIM Data Governance Maturity Model.....	56
4.6.2	Kalido Data Governance Maturity Model	58
4.6.3	IBM Data Governance Council Maturity Model	59
4.7	Data Governance Frameworks.....	59
4.7.1	Data Governance Institute Framework	59
4.7.2	Data Management Association (DAMA) Framework	61
4.7.3	IBM Data Governance Council Framework.....	62
4.8	Data Stewardship	63
4.9	Assessment of Maturity Levels of Agencies	64
4.10	Policies and Procedures.....	66
4.11	Recommended Approach for Data Governance.....	70
5	Referenced Documents	70
5.1	Government Documents.....	70
5.2	Non-Government Documents.....	72
6	ACRONYMS	72
	APPENDIX A: AS-IS SYSTEM OVERVIEW.....	A-1
	APPENDIX A-1: SUPPORTING DOCUMENTATION.....	A-1-1 thru A-1-15
	APPENDIX B: PROGRAM MATRIX.....	B-1

List of Tables

Table 1: Goals/Objectives of the TO-BE System	1
Table 2: Outcomes.....	2
Table 3: Exploration Questions/Answers.....	2
Table 4: Information View Artifact	19
Table 5: MITA Conditions and Standards/NHSIA Features.....	33
Table 6: Matching Criteria	40
Table 7: Gartner EIM Data Governance Maturity Model	57
Table 8: Assessment result on data governance maturity level	65

List of Figures

Figure 1: AS-IS System Overview.....	15
Figure 2: AS-IS System Overview.....	16
Figure 3: NHSIA Viewpoints.....	18
Figure 4: Standardization Data Moving Across Systems.....	21
Figure 5: NIEM Governance Structure	22
Figure 6: NIEM HS Domain Governance Structure.....	23
Figure 7: NIEM-UML: PIM & PSM Perspectives	26
Figure 8: Components of NIEM-UML Specification.....	27
Figure 9: NIEM-UML Profiles	28
Figure 10: MITA Framework.....	29
Figure 11: MITA Governance Structure.....	29
Figure 12: MITA Framework.....	30
Figure 13: Federal Enterprise Architecture (FEA)	33
Figure 14: IBM MDM Logical System Architecture.....	37
Figure 15: Example Mapping RA to IBM Tools	38
Figure 16: Interoperability using matching criteria with MDM for eMPI.....	41
Figure 17: Interoperability using a Hybrid Approach for MDM and eMPI.....	42
Figure 18: Interoperability using Registry Approach for MDM and eMPI.....	43
Figure 19: Data Flow Process	45
Figure 20: Security Vision	47
Figure 21: GFIPM Exchange Security	48
Figure 22: Data Governance	50
Figure 23: State of Oklahoma Enterprise IT Governance Model.....	53
Figure 24: State of Oklahoma's Current Governance Structure	54
Figure 25: Recommendation for TO-BE Data Governance Structure.....	55
Figure 26: Data Governance Components.....	56
Figure 27: Kalido Data Governance Model	58
Figure 28: IBM Data Governance Council Maturity Model	59
Figure 29: Data Governance Institute (DGI) Framework.....	60
Figure 30: DAMA Functional Framework	61
Figure 31: DAMA Environmental Framework	62
Figure 32: IBM Data Governance Framework.....	63

1 EXECUTIVE SUMMARY

1.1 Purpose

Develop a roadmap for a fully integrated, reusable, deduplicated (whenever possible) data exchange for reports and all services exchanged between Oklahoma Department of Human Services (OKDHS), Oklahoma Health Care Authority (OHCA), Oklahoma State Department of Health (OSDH) and other initiatives. The roadmap will focus on the Enterprise Master Person Index (eMPI) and eligibility requirements. This roadmap includes the data these systems will share in inter-agency collaboration by using the National Information Exchange Model (NIEM) for a consistent and repeatable exchange of data between systems and agencies through the integration of information via an enterprise data warehouse and web services.

This project will provide opportunities for inter-agency collaboration and allow multiple State agencies to leverage Service Oriented Architecture (SOA) services and capabilities, in support of the state’s effort to meet the timelines of the Affordable Care Act (ACA) for citizen enrollment.

1.1.1 Goals/Objectives

The major goals/objectives to be achieved with the implementation of the TO-BE system are summarized in Table 1.

Table 1: Goals/Objectives of the TO-BE System

Goal/Objective	Desired Outcome	Measurement	Impact
Standardization	Enterprise wide standards	Adopted by Inter/Intra Agencies and Programs	Improved efficiency
Reusability	Shared & reused data	Adopted as a model by other states	Reduction of development time
Reduce Data Redundancy	Data Consistency	Adopted by Inter/Intra Agencies and Programs	Improved data integrity and reduced errors
Governance	Policies and Procedures	Adopted by Inter/Intra Agencies and Programs	Conformance to standards
NHSIA Compliancy	Compliance with national Architecture Framework	Adopted by Inter/Intra Agencies and Programs	Achieve interoperability
Compliance to NIEM Framework	Compliance with national Architecture Framework	Adopted by Inter/Intra Agencies and Programs	Achieve data/service interoperability
Compliance to MITA	Compliance with National Architecture Framework	Adopted by Inter/Intra Agencies and Programs	Achieve interoperability

1.1.2 Project Outcomes

The proposed interoperability plan provides the maximum potential for mutual benefit and “reusability” by health and human services organizations in Oklahoma, enabled through the Project Outcomes listed in Table 2.

Table 2: Outcomes

Index	Project Outcome
O1	The outcome of this document will be to provide an initial roadmap that will lay the ground work for further investigation and will integrate with the roadmap for SOA/Enterprise Service Bus (ESB) to allow fully automated data exchange and service reusability for all services exchanged between OKDHS and OHCA and other initiatives.
O2	Another outcome of this document will provide a data roadmap that can be used by other states.
O3	A third outcome of this document is that it will provide the framework for the implementation of an eMPI system.
O4	Provide Enterprise-Wide Data Definitions and Data Repository starting with eMPI focus; thus building groundwork for covering other areas.

1.2 Background/Overview

Data Roadmap will be a collaborative effort consisting of a partnership between the Office of Management and Enterprise Services (OMES), OKDHS, OSDH and the OHCA to improve both the quality and efficiency of data exchange.

Currently OSDH is working independently on one interoperability plan, while OHCA is working on another interoperability plan and OKDHS is developing third one. These inefficiencies are creating disjointed plans. The intent is to come up with a unified overall interoperability process that can improve data exchange processes, increase data quality and reusability, and/or reduce errors and enhance data integrity between all the agencies.

1.2.1 Exploration Questions/Answers

This plan in conjunction with the plans covered under this grant will seek to explore and answer the following questions in Table 3.

Table 3: Exploration Questions/Answers

Index	Exploration Questions/Answers
Q1	What resources will be needed to integrate OKDHS human services programs into Medicaid Information Technology Architecture (MITA) Maturity Model (MITA Framework Version 3.0)/National Human Services Interoperability Architecture (NHSIA) compliant architecture?
A1	From Data Architecture perspective, Data Architect, Data Modeler, Database Administrators, Security Architects, Business Analyst, Business Architects, experienced XML Developer, Business Liaison, Program Manager, Stakeholder participation, executive level participation for data governance, and resources from NIEM/NHSIA.
Q2	What technical and business architecture will be needed at OKDHS to integrate MITA? What is the security architecture that protects the interests of all State agencies?
A2	{To be addressed in further deliverables}
Q3	What is needed among the health and human services agencies to develop and share eMPI?
A3	The participating agencies were questioned as to the matching criteria that they use in their systems to identify a person. Except OSDH, for all other agencies applying the MDM technology to leverage the eMPI concept by storing them in a master data for

Index	Exploration Questions/Answers
	ease of access and sharing, and thus reducing the errors and maintenance cost of the stored data, would be a valuable asset when focusing on eMPI for interoperability. OSDH has a state mandate that the Birth information is only released to certain designated agencies and their data cannot be shared for eMPI purposes.
Q4	What initiatives of the MOSAIC human services eligibility and case management system can be shared with OHCA initiatives under the Affordable Care Act?
A4	The effort towards the design of MOSAIC may be utilized to some extent for the enterprise-wide interoperability since MOSAIC covers the interoperability between three big OKDHS lines of business.
Q5	What efficiencies can be gained by using SOA?
A5	<p>The SOA will give us a more agile environment and can transform the IT landscape by increasing efficiencies and decreasing costs.</p> <p>Efficiency = output/input*100</p> <ol style="list-style-type: none"> 1) Efficiency operates within the context of other performance measures like effectiveness, return on investment etc. 2) Efficiency must be measured relative to a standard – the ideal point before efficiency becomes a negative measure.
Q6	How can governance be used to achieve the wide range of performance expectations?
A6	<p>Governance refers to the means for achieving direction, control, and coordination. Data governance enables high performance because it is a key component in effective information management. Following are the most important characteristics to support a successful data governance implementation:</p> <ol style="list-style-type: none"> 1) The business case for data governance should be established early on and is used to guide the prioritization of data governance implementation. Metrics should be identified that enable measurement of the business benefits delivered. 2) The approach to data governance accounts for the people, process and technology aspects. This shows that data governance is as much about leadership, communication and good management as it is about technical integration. 3) The implementation of data governance should be planned as a journey, with distinct phases reflecting an organization's evolution along the spectrum of information management maturity. 4) Realistic expectations should be set about the benefits, timelines and capabilities associated with data governance. 5) Data governance should be tackled within the context of a comprehensive data management approach that also addresses data architecture, metadata and data structure, MDM, data quality and data security.
Q7	How can Oklahoma improve overall State IT operating and cost efficiencies?
A7	<p>Using the SOA Architecture integrated with MDM technology for the overall architecture and using NIEM to leverage NHSIA for data exchanges Oklahoma will significantly reduce cost of maintenance of data and services.</p> <ol style="list-style-type: none"> 1) MDM will provide a one stop shop for eMPI data that will lower the maintenance costs, provide high performance scalable system thus resulting in better services to the customers: Good Service, Happy Customers. 2) Using NIEM for data exchanges will allow disparate systems to talk in one language. It creates a seamless transfer of information instead of a point-to-point architecture. Point-to-point architecture is hard to maintain and any

Index	Exploration Questions/Answers
	change would prove to be more costly than if we were following a predefined process defined by an existing framework that is proven to work for governments. It provides a more agile system and since it's based on SOA, implementing changes would be easier, less time consuming and would lead to cost avoidance for the state.

1.2.2 Options Considered

Based upon the Information Exchanges as is defined in the National Human Services Interoperability Architecture (NHSIA) Information Viewpoint, current information exchanges will be mapped to fit in NHSIA's information exchanges and leveraged through NIEM-UML (Unified Modeling Language). Oklahoma has chosen to adopt NHSIA and MITA as standards for requirements with the partnership being established for Interoperability. In the event NHSIA does not address a process, MITA will be used. The governing body for data exchanges will be NIEM Human Services (HS) Domain Governance. Inter-agency and intra-agency specific data governance is taken into consideration in this roadmap.

1.2.2.1 Master Data Management for eMPI

Some of the options that were taken into account while working on a solution towards eMPI are given below in Option 1, Option 2, and Option 3:

Option 1: Repository Approach

The repository approach will use the person matching criteria as an eMPI focus.

One current constraint to this approach includes: OSDH Birth Certificate (BC) data cannot be currently included in the eMPI (e.g. a shared data repository) but may be available in a restricted manner in the future, pending applicable approvals.

Option 2: Hybrid Approach

The hybrid approach will allow each agency the option to retain their current MPI system, but still allow other agencies to use the matching criteria for creating a Master Person Data Management (MPDM) system. With this approach, the MPDM will have a unique identifier that maps back to each agency.

Option 3: Registry Approach

The registry approach will create an MPDM hub that contains a list of keys that can be used to find all the related records for a particular master data item. For example, if there are records for a particular client in the databases of OSDH and OHCA, and OKDHS which includes: Adult and Family Services (AFS), Child Welfare Services (CWS), Oklahoma Child Support Services (OCSS), the MPDM hub will contain a mapping of the

keys for these records to a common key. In this case the eMPI will be focused on a unique identifier for a person across all agencies.

1.2.2.2 Potential Tools

MPDM is a subset of Master Data Management (MDM). MPDM products can be bought and customized or built in-house.

1.2.2.2.1 Potential eMPI Tool:

- IBM® Initiate®

1.2.2.2.2 Potential MDM Tools:

- IBM Infosphere Master Data Management
- OneData Master Data Management from Software AG
- TIBCO Master Data Management

1.2.2.2.3 Potential NIEM Tools:

- **OASIS Content Assembly Message (CAM)/jCAM:** The open source OASIS CAM/jCAM toolkit provides a selection of tools that directly support NIEM. The CAM toolkit supports end to end development of NIEM Information Exchange Package Documentation (IEPD's) from inception to delivery of completed XML Schema Definition (XSD) schema, example Extensible Markup Language (XML) test cases and business rule documentation. The open source implementation is available through the CAM processor on Sourceforge. The toolkit is an implementation of the OASIS CAM v2.0 standard. The toolkit also supports development of domain dictionaries and currently includes the LEXS dictionary along with local copies of NIEM 2.0 and NIEM 2.1 dictionaries in XML. The toolkit also supports importing enterprise data models, applying Naming and Design Rules (NDR) checks and spelling and renaming automation. An introduction to the concepts of using CAM to develop NIEM IEPDs using either dictionaries or blueprints or by ingesting existing XSD schema is available at the OASIS CAM Technical Committee (TC) documents website.
- **NIEM Wayfarer 2.1:** A tool developed by a NIEM practitioner that provides the ability to search the NIEM data model during the mapping process. NIEM Wayfarer is a preferred tool by many implementers during the search and mapping process, but is not supported by the NIEM Program Management Office (PMO), and might not reflect the most current version of NIEM. This tool is publically available on the web.
- **Justice Information Exchange Model (JIEM) modeling Tool:** The current JIEM® Reference Model is a set of information exchanges regarding business

functions that are common to most jurisdictions. So we would most likely not use this tool. More research needs to be done to check if this tool supports Health and Human Services Information Exchange.

- **NIEM SAW:** NIEM Stand-Alone Wayfarer (SAW) is a tool for exploring and searching NIEM, an XML interchange standard for federal, state, and local government information, including law-related information. This could be taken as an example if we need to build one for health and human services related information. SAW runs on a local computer.
- **Oracle SOA/BPM Suite:** Oracle SOA Suite is a SOA-enablement platform that provides organizations with a robust infrastructure to support application integration, service orchestration, business process management, and messaging. Business Process Management (BPM) capability with human workflow support can be purchased as an add-on to the SOA Suite.

1.2.2.2.4 Potential Tools for Data Governance:

Data Governance software generally falls into three categories:

- Team workspaces
- Repositories holding policies, business rules, data definitions, metadata
- Data Management, MDM, Extract Transform and Load (ETL), or Data Quality software that includes governance or stewardship functionality

Various Data Governance tools are available based on the 3 categories defined above.

- **DataVersity Data Governance Office (DGO):** DataVersity DGO is a federated data governance tool that is built upon the proven data governance framework and methodology of Data Governance Institute (DGI). It walks you through the five fundamentals of creating and managing a data governance office through a centralized, collaborative team space. It also offers the option of collaboration with peers and mentors for guidance through all phases. DGO provides an integrated system of data governance with built-in guidance, methodology and workspace processes to make the establishment and management of a workable data governance program both feasible and cost effective.

DATAVERSITY DGO Pricing:

- Starter \$195 (Single User)
 - Essentials \$385 (Single Team/Unlimited Users)
 - Expansion \$685 (Unlimited Teams/Unlimited Users)
 - Enterprise \$2,485 (Dedicated Hosting/Network Appliance Option)
- **Computer Associates (CA) Erwin Web Portal:** The CA Erwin web portal provides a simple, customizable, web-based interface that allows both business and technical users across the organization to easily visualize the important metadata information that is stored in CA Erwin data modeler. While only certain users will want to view or create data models, many more users need access to

the information in those models, but would like this information presented in an intuitive and easily accessible way. The CA Erwin web portal allows easy access to information via the web, with a variety of presentation and search formats to cater to a wide range of user types in the organization. This tool will be valuable for assessment of the widespread data that we will be dealing with across the organizations. It will provide visibility and show the discrepancies of between the naming conventions used by the agencies for the same purposes. It will be a big asset towards reducing redundancies and anomalies and helps do the analysis for a streamlined database. The Enterprise Edition runs on Oracle, SQL Server 2008 and uses a single-sign on authentication. The cost for this tool is roughly:

CA Erwin Web Portal Approximate Pricing:

- 1–25 Users: \$23,000–\$27,000
- 25–50 Users: \$41,000–\$48,000

The actual cost may be less since we qualify for government discounts. CA also offers tools for Data Profiling that is a Data Quality tool.

- **IBM® Initiate® Inspector™:** Inspects data, visualizes relationships, and collaborates to resolve issues.
 - Gives organizations new and meaningful insights and views of their data.
 - Exposes complex relationships within data.
 - Easy to deploy and cost-effective.
 - A data governance and stewardship application that alerts to potential data quality issues and gives them tools to resolve these issues.
 - Helps distribute the workload to the most appropriate resources.
 - Unlike other competitive offerings, IBM® Initiate® Inspector™ is designed for the needs of data stewards.
- **Kalido Data Governance Director:** Kalido Data Governance Director helps improve the data used in business processes through data policy management. It allows easy view data from a process perspective, the context of how they are used in a business process, and a technical representation, facilitating a shared understanding of where data is within the enterprise and how it is consumed.
- **Informatica Solution for Data Governance:** The Informatica solution for data governance is based on lean and agile data management principles. The solution focuses on improving data quality, protecting sensitive data, promoting the efficient sharing of information, providing trusted business–critical data, and managing information throughout its lifecycle. This unique approach to data governance is underwritten by a set of implementation best practices that minimize risk and deliver business value quickly.
- **Oracle Data Governance Manager (DGM):** Oracle DGM serves as a place to define and set enterprise master data policies and to monitor and fix data issues. It

also helps operate the different functions in the MDM data lifecycle: Consolidate, Master, Cleanse, Share and Govern, and is designed around these functions.

- **Trillium Software (TS) System Insight:** TS Insight gives all users, from executive management to focused analysts to engineers, visibility into the level of quality and the compliance of data to corporate standards across varying systems and applications. TS Insight presents data quality metrics in intuitive graphical forms that help data quality team members, data stewards, and data governance committees monitor the status of data and understand how it impacts enterprise goals. Through their web browsers, users track and visualize the status of data quality within the organization in an accurate and timely report.

TS Insight is a web-based, data quality dashboard complete with scorecards that allow users to:

- Monitor the compliance of data that streams in from different sources.
 - Track data conformance over time to understand its impact on reporting accuracy and decision making.
 - Compare third-party data, capture unexpected changes and prevent havoc in operational systems.
- **IBM Rational System Architect (SA)**

1.2.3 Options Impact and Goals

1.2.3.1 Improve Service Delivery for Clients

The implementation of SOA along with MDM technology supports the business needs across state agencies and benefits the client in several ways by:

- Reducing the amount of documentation families must submit to apply for multiple benefits
- Reducing the time spent by families applying or retaining eligibility
- Providing accurate, reusable and easily accessible services
- Reducing errors by increasing efficiency and improving performance
- Reducing customer dissatisfaction by supplying readily available information

The eligibility determination is currently a mix of processes; there are manual and electronic processes for the various federal social service programs that are integrated only through custom interfaces with no exchange standards. No standard electronic application currently exists that can be used across multiple public assistance programs. An interoperable, reusable eligibility system will help bridge this gap. This improvement can be enabled by not only leveraging the evolving Oklahoma enterprise SOA framework, but also the governance strategy to facilitate proper design and execution of a prospective enterprise workflow. This use case also provides an opportunity to explore

how additional efficiencies can be achieved to meet the ACA Gold Standard User Experience, where clients are automatically referred to appropriate services.

Determining Eligibility Under Affordable Care Act – The ACA Gold Standard User Experience refers to an improved Eligibility System for customer satisfaction. As is stated in the “Guidance for Exchange and Medicaid Information Technology (IT) Systems” by CMS, Eligibility Process should be a streamlined, secure, and interactive customer experience that will maximize automation and real-time adjudication while protecting privacy and personally identifiable information.

Eligibility process should encapsulate the following functionalities:

- Individuals will answer a defined and limited set of questions to begin the process, supported by navigation tools and windows that open to provide or seek additional information based on individual preferences or answers.
- The application will allow an individual to accept or decline screening for financial assistance, and tailor the rest of the eligibility and enrollment process accordingly.
- The required verifications that will be necessary to validate the accuracy of information supplied by applicants will be managed in a standardized fashion, supported by a common, federally managed data services hub that will supply information regarding citizenship, immigration status, and federal tax information.
- Tools for calculation of advance premium tax credits will also be provided.
- Business rules will be supplied that will allow for resolution of most discrepancies through automation, including explanations of discrepancies for the consumer, opportunities to correct information or explain discrepancies, and hierarchies to deal with conflicts based on source of information and extent and impact of conflicts on eligibility.
- Individuals will attest to the accuracy of the information they supply.

The goal is to serve a high proportion of individuals seeking health coverage and financial support through this automated process.

1.2.3.2 Reduce Errors and Improve Program Integrity

A critical challenge to realize an enterprise solution for the Eligibility Use Case is a common and accurate way of identifying clients, which is consistent across agencies. Oklahoma does not currently have a statewide eMPI; the addition of an eMPI will aid all agencies data steward functions when attempting to align persons across systems.

For example, currently, multiple identifiers exist for eligibility determination for, the Insure Oklahoma (IO) members, including a member ID (an OKDHS identifier) and an IO case ID (an Insure Oklahoma identifier). In the current workflow where manual reference checks are performed, the opportunity for errors increases. Through the development of an eMPI:

- Errors can be reduced
- Accuracy of eligibility determinations increased

Using the MDM, all eMPI focused data will be stored in one location, which will be maintained in a regular basis thus reducing the chance of pulling erroneous information. Information reported to or available in one program can be shared with other programs in support of program integrity efforts.

1.2.3.3 Improve Administrative Efficiency

Addressed across the Interoperability Plan tiers, performance improvements can be realized through the development of business processes, enabled by SOA, which can automatically perform eligibility validation and cross-referencing, as web services are enabled across the enterprise. Through the SOA Roadmap, the development of business processes and the validation performed by web services to support these processes, administrative activities can be transformed to reduce redundancy of effort and streamline workflows.

2 SCOPE

The scope of this document is focused on interfaces/data exchanges between agencies and not the systems/subsystems. The interfaces could be real time or set for some intervals of time. It will cover the data exchange that involves eligibility and enrollment with a focus on eMPI. See Appendix B-1 for the list of interfaces.

2.1 Options Enterprise Architecture and/or Modules

The architecture for interoperability will focus on NHSIA framework using NIEM to implement SOA architecture for data exchanges. Enterprise Service Bus could be a COTS product or a series of products that supports communication between reusable services for data exchanges. Since MITA is more mature compared to NHSIA, MITA elements could be pulled in to fill in the gaps that NHSIA does not have a strong hold on.

2.2 End Result

Best practices will be taken into consideration to achieve maximum efficiency with interoperability. The results of cost benefit analysis and thorough assessment and gap analysis could be a factor that could bring a change to the proposed approach.

2.3 Breadth

The focus of this interoperability effort will include: state and federal programs that require eligibility determination: Federal Supplemental Nutrition Assistance Program (SNAP), Temporary Assistance for Needy Families (TANF), Low-Income Home Energy Assistance Program (LIHEAP), Aid to the Aged, Blind and Disabled, and the child care subsidy. Other human services programs that will benefit from a new configuration of IT services

include Child Welfare, Child Support Services, Aging Services Division (Medicaid funded long term care waiver) and Developmental Disabilities Services (Medicaid funded community based waivers). Other state agencies that are participating in the consortium include OHCA, Oklahoma Department of Mental Health and Substance Abuse Services and Oklahoma State Department of Health's program; Women, Infants and Children (WIC). Other business segments involved in planning include the Department of Public Safety and the State Department of Education.

2.4 Human Services Program and Initiatives

OKDHS is undertaking a multi-year, multi-program, agency-wide effort to update its technology, streamline and improve its business practices, consolidate its information systems, and provide a secure, compliant Web portal for OKDHS employees, clients and providers to conduct daily business...anytime, anywhere. OKDHS is pursuing a new Enterprise Software solution that is flexible and supports interoperability to allow internal and external stakeholder's access to the Enterprise System and data, regardless of technology. OKDHS is seeking an Enterprise Software solution that will increase client use of self-service tools. The project will lead to a fully-functional, automated system that meets federal certification, compliance and mandates for child support, child welfare, and adult and family services and the associated titles and certifications needed for certification.

2.5 Information Technology Initiatives

OKDHS is working with state governance and leadership to procure the software, installation and configuration for an enterprise human services application (HSA) to support the core business functions and processes of OKDHS, as described for the Enterprise System. Also, the OHCA is seeking to implement the technical aspects of the Affordable Care Act for Oklahoma. Many aspects of the OHCA plan are consistent with the approach envisioned by the model. OHCA and OKDHS are working together on both of their initiatives to assure no duplication in funding or resources for similar projects using the MITA and NHSIA principles of re-usability. The proposed system will:

- Modernize existing system functionality to provide recipients a "golden standard" of customer care (i.e., a consistent look and feel across stakeholders and seamless customer service with consistent metrics to measure and continuously approve the customer experience).
- Significantly enhance the ability for providers to have prompt access to member eligibility and enrollment information to ensure that eligible individuals receive the health care benefits to which they are entitled and that providers are reimbursed promptly and efficiently.

An individual seeking health coverage in 2014 will be able to access information and assistance, and apply for health coverage, through multiple channels. All of these channels will connect with a standardized, web-based system to evaluate the individual's eligibility for coverage through one of four programs:

Qualified health plans through the Exchange (with or without Guidance for Exchange and Medicaid Information Technology (IT) Systems 4 Version 2.0 May, 2011/Centers for Medicare & Medicaid Services advance premium tax credits and cost-sharing reductions).

- Medicaid
- CHIP
- Basic Health Program, if established by the state

MITA ensures the availability of high-quality health care coverage to families and individuals who are achieved through a collaborative partnership between and within federal agencies and states responsible for implementation of the Exchanges and the Affordable Care Act's Medicaid and CHIP provisions.

MITA envisions a streamlined, secure, and interactive customer experience that will maximize automation and real-time adjudication while protecting privacy and personally identifiable information. Individuals will answer a defined and limited set of questions to begin the process, supported by navigation tools and windows that open to provide or seek additional information based on individual preferences or answers. The application will allow an individual to accept or decline screening for financial assistance, and tailor the rest of the eligibility and enrollment process accordingly. The required verifications that will be necessary to validate the accuracy of information supplied by applicants will be managed in a standardized fashion, supported by a common, federally managed data services hub that will supply information regarding citizenship, immigration status, and federal tax information. Tools for calculation of advance premium tax credits will also be provided. Business rules will be supplied that will allow for resolution of most discrepancies through automation, including explanations of discrepancies for the consumer, opportunities to correct information or explain discrepancies, and hierarchies to deal with conflicts based on source of information and extent and impact of conflicts on eligibility. Individuals will attest to the accuracy of the information they supply. The goal of MITA is to serve a high proportion of individuals seeking health coverage and financial support through this automated process.

2.6 Health Intersection

Frameworks MITA and NHSIA were taken into consideration to achieve interoperability for eligibility services. During research it was found that NHSIA is aligned with MITA. The roadmap takes these findings into consideration and plans to work with NHSIA framework since it's more geared towards Human Services; however understanding that MITA is more mature than NHSIA in certain aspects, the roadmap gives an option to use MITA in such cases where NHSIA is struggling.

2.7 Assumptions and Constraints

- **Schedule Constraints:** Delayed start on Interoperability Planning Grant, the schedule is contingent upon approval of SOA Roadmap. Currently separate agencies, divisions and programs have different schedules for upgrading systems

and infrastructure based on immediate needs, federal rules and available funding. Agencies are in different stages of the process. For example one is planning, one has an RFP out and the other is in progress.

- **Data Constraints:** Focusing on Eligibility and eMPI, initially on data exchange between agencies/programs.
 - ✓ Currently OCSS, OKDHS, OHCA, OSDH each have and use their own intake for services and MPI process. This is a business data constraint because we collect different information in different ways for different purposes but need to share that information between when we have common customers.
 - ✓ OKDHS, OHCA and OSDH have requirements to have interagency data sharing agreements. This is a constraint because it takes on a lengthy path through business, legal and executive reviews and approvals.
 - ✓ OKDHS, OHCA, OSDH and our federal partners have similar or same data but different data definitions.
- **Hardware Constraints:** Any required hardware must fit with SOA and Enterprise Architecture, and acquisition of any additional hardware is dependent on funding or financial constraint.
- **Software Constraints:** Any required developed or COTS software must fit within the approved SOA and Enterprise Architecture, and acquisition of any additional software is dependent on funding or financial constraint.
 - ✓ Not only does our organizations not use any common COTS product to share business data or processes we have varying degrees of software applications and languages in each internal organization.
- **Organizational Constraints:** Resource acquisition and allocation may be a factor in implementing the Interoperability Plan. Policies and procedures may be too specific to share or reuse for purposes other than eligibility. OSDH cannot share Vital Records as an eMPI by State mandate, but could be shared in the future based state and legal agreements.
 - ✓ Each organization uses their own data center and resources to manage and support the hardware and software that support the organizations business data and processes. In addition by having varying types of hardware and software requires different types of resources and skills sets to maintain theses.
 - ✓ Business process changes that may be required to implement the interoperability plan will likely meet with resistance from affected staff in each organization.
 - ✓ Funding streams often dictate specific guidelines, policies, systems, etc, and we may not be able to influence change with the respective Federal agencies. In the interim, we must be compliant with federal funding terms and conditions.
 - ✓ Some agencies may have some systems that are considered proprietary by a vender.
 - ✓ Some policies and practices are based in State and Federal law which govern accessibility to data.
- **Security Constraints:** The regulations of the Internal Revenue Service (IRS), HIPAA, and Social Security Administration (SSA) must be considered. Compliance with Federal and State Mandates for Accessibility, Compliance with Program

requirements for Confidentiality, Compliance with Federal and State Mandates, as well as IT Standards for the creation, storage, reading and transfer of data need to be taken into consideration.

- **Political Constraints:** Local, state or federal mandates may impose constraints.
- **General Constraints:** Federal funding streams earmarked to certain programs with attached restrictions and regulations create artificial silos creating barriers to achieving interoperability across various human service organizations and programs. In a sense, this barrier makes it difficult for certain organizations to “break out” of their current silos; although the Memorandum of Agreements (MOU) and Service Level Agreements (SLA) between organizations attempt to solve some of these issues, this barrier is ever present based on the pure mechanics. As implementation of the NHSIA Business Viewpoint strives interoperability through a functional point of view so must go the federal funding streams and associated restrictions and regulations if true interoperability is to be archived.

The partnership is committed to the development of a roadmap for integration of Service Oriented Architecture (SOA)/Enterprise Service Bus (ESB) to allow fully automated data exchange and service reusability for all services exchanged between OKDHS, OSDH and OHCA and other initiatives.

The partnership is also committed to the development of a model for the use of the National Information Exchange Model (NIEM) to enable a consistent exchange of data.

2.8 Benefit to Other States

This Interoperability Plan can be used by other states to implement Enterprise Interoperability measures. This roadmap uses the national standards for data exchanges. States interested in eligibility and enrollment can benefit from this roadmap because it provides a roadmap for implementing SOA architecture using NHSIA and NIEM focusing on eMPI. MITA framework has been taken into consideration for cases where NHSIA might not cover some piece of Health information exchange. It also suggests some COTS products that could be used for implementing the SOA architecture. An example of an eMPI implementation design is provided that could provide a basis while considering different approaches to eMPI.

- Roadmap: Collect the AS-IS information exchange, Interface names, descriptions of data exchange, source, destination, and data elements
- Map the AS-IS Information exchanges to NHSIA Information Exchanges
- Leverage NHSIA through NIEM

3 APPROACH

3.1 AS-IS Overview

Figure 1 shows the interactions between Oklahoma Department of Human Services (OKDHS) agencies (e.g., PS2 - Adult and Family Services (AFS), Oklahoma Support

Information System (OSIS) - Oklahoma Child Support Services (OCSS), KIDS – Child Welfare Support (CWS)), and other departments and organizations (e.g., OHCA - Medicaid Management Information System (MMIS), Office of Management and Enterprise Services (OMES), Oklahoma State Department of Health (OSDH)).

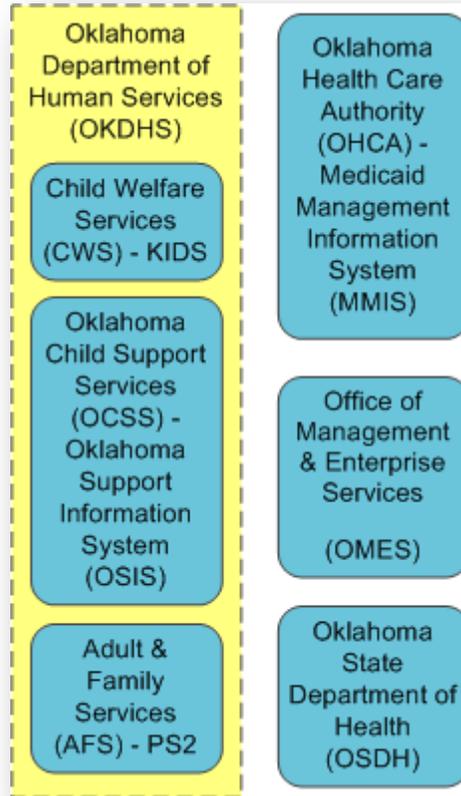


Figure 1: AS-IS System Overview

Figure 2 illustrates the AS-IS data exchanges among agencies with a focus on Eligibility and Enrollment.

90FQ0006 Oklahoma Interoperability Grant Project
 Data Road Map, Revision 2.0, April 26, 2013

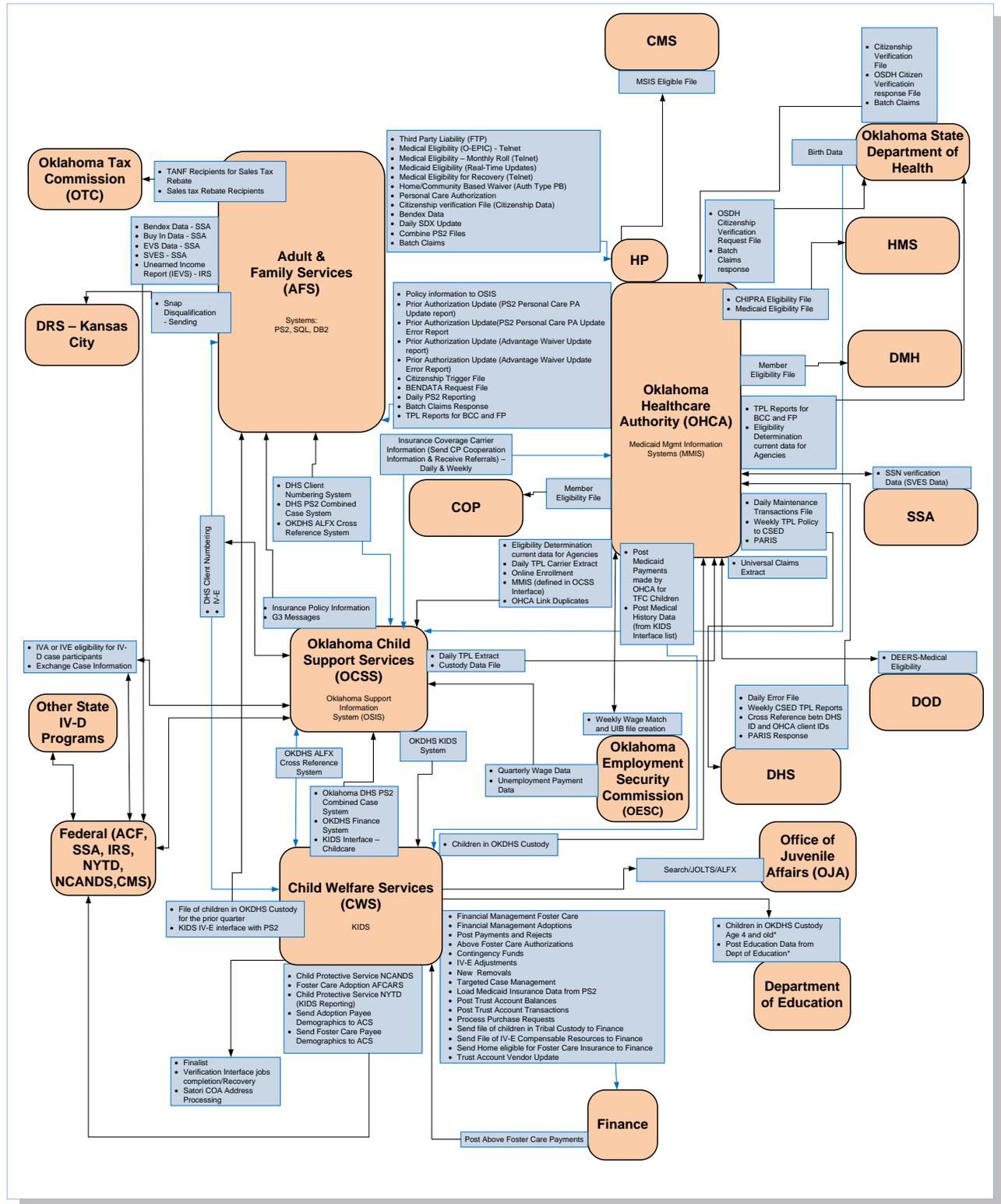


Figure 2: AS-IS System Overview

- OCSS – OSIS is an automated system developed to assist OCSS in administering the state’s Title IV-D of the Social Security Act program functions, including case initiation, case management, paternity and order establishment, cash and medical support enforcement, financial management, interstate case processing, locate, security and reporting.
- AFS – PS2 is the case information and data management system. It is a major client services system. Family Assistance and Client Services (FACS) is the Graphical User Interface (GUI) “front end” to the PS2 System.
- CWS – KIDS is a Statewide Automated Child Welfare Information Systems (SACWIS). SACWIS is a comprehensive automated case management tool that supports social workers in foster care and adoptions case management.
- OHCA – MMIS is a highly sophisticated, feature-rich system centered on a strong, Medicaid-specific relational data model.
- OSDH – Public Health Oklahoma Client Information System (PHOCIS) supports client services.

The AS-IS detailed overview for the systems identified above can be found in Appendix A.

3.2 TO-BE System

The TO-BE System will take into consideration the MITA framework, NHSIA framework and NIEM. NHSIA shares eligibility determination process with Centers for Medicare and Medicaid Services (CMS). One of the seven conditions that are built into MITA is that it be interoperable with human services. NHSIA has built a compatible architecture that together is going to help states implement the ACA across their Health and Human Services programs and systems. NHSIA architecture is broken down into seven different viewpoints, one of them is the Information Viewpoint, and that employs NIEM in the development of the architecture.

MITA framework uses UML – based standard – HL7 for Health Information Exchanges (HIE). NIEM released a beta version of NIEM-UML, which is a Model Driven Architecture (MDA) for NIEM Information Exchanges. NIEM-UML extends and tailors the unified modeling language. NIEM-UML represents collaboration between the Object Management Group (OMG) and NIEM communities.

This roadmap will focus on plans to implement NHSIA framework and will use MITA framework to cover the gaps if any missing pieces are identified.

3.2.1 National Human Services Interoperability Architecture (NHSIA)

NHSIA is a framework to support integrated eligibility determination and information sharing across programs and agencies, improved delivery of services, prevention of fraud, and better outcomes for children and families. It consists of business, information, and technology models to guide programs, states, and localities in the efficient and effective delivery of services.

The NHSIA is built to comply with recognized security and information exchange standards for safely and securely sharing information across organizational and jurisdictional boundaries and all levels of government. The NIEM, as defined and governed by the Department of Homeland Security, is the primary standard used in building the Information Viewpoint. See Figure 3 for NHSIA Viewpoints.

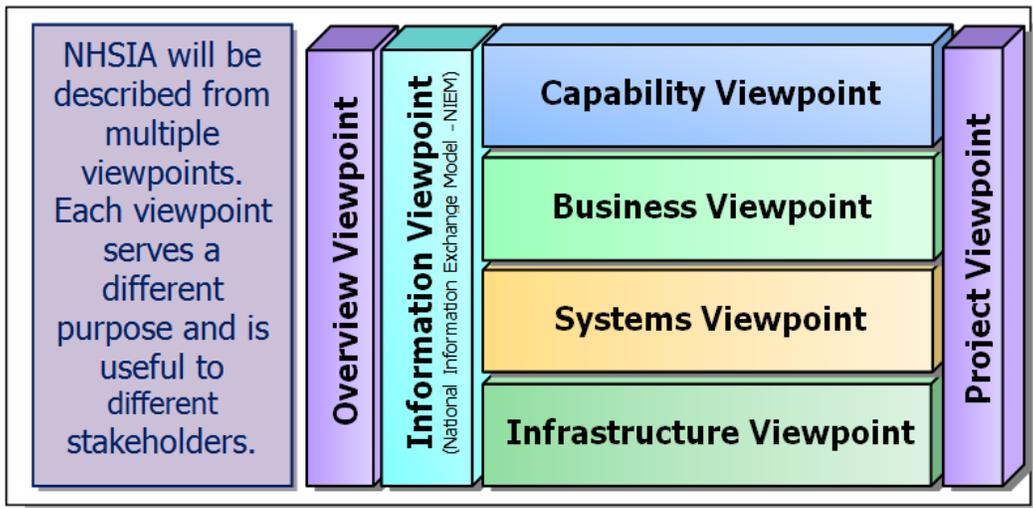


Figure 3: NHSIA Viewpoints

The Information Viewpoint products can facilitate interoperability among Human Services systems and processes in several ways:

- Alignment with the “Information Input and Output” terms defined in the Business Viewpoint Description document provides a common vocabulary for discussion of shared information.
- The NHSIA Conceptual Data Model (CDM) identifies classes, attributes, and relationships between classes at a level of detail that can guide the development of standards, while leaving some flexibility to respond to specific stakeholder needs during the standards development process.
- Development of specific NIEM Information Exchanges, including XML message schemas for the identified Information Exchanges, will support actual implementation of interoperable interfaces that can be leveraged by current and future stakeholders.
- The Information Viewpoint provides a vocabulary, requirements, and context to support the development of the Human Services Domain of the NIEM. NIEM is designed to develop, disseminate, and support enterprise-wide information exchange standards which enable federal, state, local, and tribal jurisdictions to effectively share critical information required by their operations.

3.2.1.1 NHSIA Information Viewpoint Artifacts

Below is the list of Artifacts planned to be included in Information Viewpoint, as shown in Table 4.

Table 4: Information View Artifact

Artifact	Form and Description
List of Relevant Standards	<i>Form:</i> Spreadsheet of standards with detailed descriptions.
	<i>Description:</i> A spreadsheet of existing information standards in the areas of data, coding, and exchange protocols relevant to health and human services. Includes oversight authority, definitions, and references.
Conceptual Data Model	<i>Form:</i> A data model generated in Enterprise Architect (EA), delivered in native EA format and as a portable document format (pdf) diagram.
	<i>Description:</i> A diagram identifying classes, attributes, and associations between classes. This model forms the basis for the model aspects for Information Exchanges (for IEPD Requirements Artifacts) and for Data Structures.
Data Dictionary	<i>Form:</i> A spreadsheet.
	<i>Description:</i> Definitions of data items identified in the CDM. Includes a mapping to the Information terms defined in the Business Viewpoint.
List of Information Exchanges	<i>Form:</i> Spreadsheet migrating to a modeling tool.
	<i>Description:</i> List and description of information exchanges between stakeholders, associated with business processes and activities from the Business Viewpoint.
IEPD Requirements Artifacts	<i>Form:</i> A data model generated in Enterprise Architect (EA), delivered in native EA format and as a pdf diagram, accompanied by a spreadsheet for the mapping.
	<i>Description:</i> Data Models derived from the NHSIA CDM focused on specific families of information exchanges. The spreadsheets map the CDM data elements to NIEM elements and identify potential NIEM gaps. The current NHSIA release addresses the “Eligibility and Enrollment” Information Exchanges.

1. List of Relevant Standards:

Below are the list of State and National Standards. These need to be reviewed and assessed as to what could be applicable to the project.

Standards for Data:

- **NIEM Standards:** Reference model for government enterprise-wide information exchange. Information Exchange Packages (IEPs) and the

Information Exchange Package Documents (IEPDs) that define them conform to the NIEM. Sponsored by US Department of Justice (USDOJ), Department of Health & Human Services, and Department of Homeland Security.

- **Global Justice XML Data Model (GJXDM):** Has been absorbed into NIEM Global Federated Identity and Privilege Management (GFIPM) – Implementation of federated identity for identification, authentication, privilege management and auditability.
- **CCD C32:** The HITSP Summary Documents Using HL7 Continuity of Care Document (CCD) Component describes the document content summarizing a consumer's medical status for the purpose of information exchange. The content may include administrative (e.g., registration, demographics, insurance, etc.) and clinical (problem list, medication list, allergies, test results, etc.) information. This specification defines content in order to promote interoperability between participating systems. This Component is essentially a subset of the healthcare data that has been developed for specific business Use Cases. This subset contains the minimum critical or pertinent medical information sections as specified by the business case.
- **Accredited Standards Committee (ASC):** Electronic Data Interchange (EDI) standards. Includes a specific Insurance/Health Series (INS), which supports insurance and other health-related business transactions.

Standards for Data Exchanges:

- **Web Services:** Protocol enabling the exchange of messages and conduct of business via the internet.
- **XML:** XML is a general-purpose markup computer language used for creating special purpose markup languages capable of describing many different kinds of data. Markup languages are formal annotation approaches to documents or collections of digital data that aid in identifying structure and content of representative data elements.
- **SOAP:** Protocol enabling the exchange of messages and conduct of business via the internet.

Standards for Coding:

- **CDC:** An established code set for coding ethnicity.
- **CMS:** Based on the America Medical Association's (AMA) Current Procedural Terminology (CPT). Standard coding for common processes involved in healthcare delivery. Level I outline medical procedural terminology and Level II addresses non-physician processes.

2. Conceptual Data Model: Eligibility Aspect of NHSIA Conceptual Data Model is attached as an Appendix on A-1-4.
3. Mapping to Data Dictionary: The mapping of data dictionary and NIEM is attached as an Appendix A-1-5.
4. List of Information Exchanges are attached as an Appendix A-1-1.

5. IEPD requirements artifact will be worked upon in the NIEM Roadmap.

3.2.2 National Information Exchange Model (NIEM)

NIEM, which uses the XML standard as a foundation, enables information sharing, focusing on information exchanged among organizations as part of their current or intended business practices. The NIEM exchange development methodology results in a common semantic understanding among participating organizations by using data formatted in a semantically consistent manner. NIEM will standardize content (actual data exchange standards), provide tools, and manage processes.

NIEM is built based on demonstrated success of GJXDM of USDOJ.

- A standardized data model for terms used in information exchanges between federal, state, local, and tribal government units
- A process for defining and sharing the context, structure, and elements of messages exchanged between two stakeholders
- A process for collaborative extension of the model's vocabulary

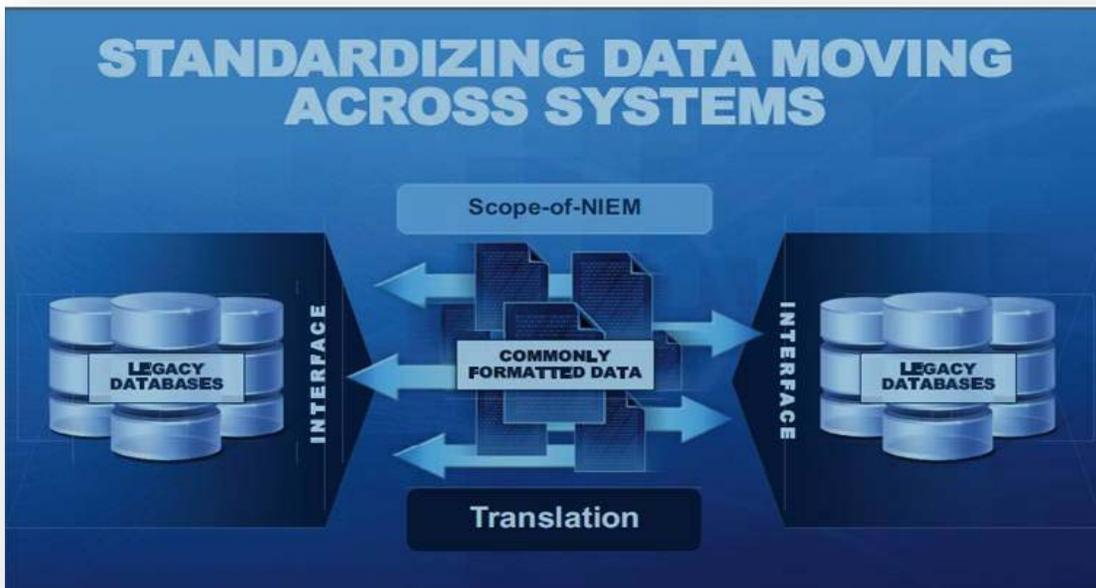


Figure 4: Standardization Data Moving Across Systems

NIEM intentionally does not address standardizing data inside legacy systems. NIEM serves as a translation layer (providing a common understanding) between and across disparate systems, as shown in Figure 4.

3.2.2.1 NIEM Governance

The NIEM Executive Steering Committee (ESC) represents key public decision makers from local, state, tribal, and federal agencies with a significant vested interest in NIEM objectives. The ESC provides strategic direction to the PMO, whose responsibilities are to oversee the implementation and development of NIEM, as shown in Figure 5.



Figure 5: NIEM Governance Structure

NIEM is jointly managed at an executive level by the Department of Homeland Security, USDOJ, and Department of Health and Human Services (HHS).

Things to consider when using NIEM for data exchanges:

- Cost Benefit Analysis of implementing NIEM for data exchanges
- Business Drivers and programmatic linkages for data exchanges between them
- NIEM trainings on the processes, available tools and Enterprise Data Management Best Practices, to meet the needs for increased education
- Collection and formalization of necessary information to be supplied to the NIEM PMO

The NIEM HS Domain is a component of a larger human services movement toward interoperability. Administration for Children and Families (ACF) is including human service programs in new interoperable systems being created through the ACA. The ACF is deeply committed to interoperability and helping build linkages between human services and ACA to improve client outcomes, lower costs and enhance operational efficiency. The use of NIEM for exchanges of information across the human service sector and beyond will be a key element of interoperability.

ACF has been authorized by the HHS Office of the Chief Information Officer (OCIO) to be the NIEM HS Domain Steward. Within ACF, the Office of Child Support Enforcement (OCSE) has been assigned responsibility for managing and implementing the tasks associated with the ACF Interoperability Initiative, including the development of the NIEM HS Domain.

3.2.2.2 NIEM Human Services (HS) Domain Overview

The purpose of the NIEM HS Domain is to support information sharing and promote interoperability between and beyond social service providers at the federal, state, tribal and local levels.

The NIEM HS Domain tools and processes will also serve as a reusable resource for new exchange development efforts so that content can be modeled in an agile but interoperable manner.

NIEM domain governance is accomplished using a federated model. In this model, NIEM governing structures provide the governance for the NIEM core and delegate governance of the individual domains to the domain's governance body. Figure 6 below shows the top level relationship between the NIEM core governing structures and the NIEM HS Domain governance body.

3.2.2.3 NIEM Human Services (HS) Domain Governance Structure

The NIEM HS Domain organization structure (Figure 6) facilitates the governance of the constituents in the community who will be developing or using the data with respect to the following:

- NIEM HS Domain data exchange model
- NIEM HS Domain IEPD's, State Systems Portal (SSP's), Model Package Description (MPD's), Business Information Exchange Component (BIEC's)
- Establishing NIEM HS Domain data exchanges
- NIEM HS Domains Adoption, Outreach and Communications



Figure 6: NIEM HS Domain Governance Structure

The governance structure consists of a Domain Steward Manager (DSM) and a NIEM HS Domain Governance Board and associated workgroups.

Membership will be a combination of federal, state, local, and tribal representatives. These representatives will be chosen to provide a combination of programmatic, policy, business and technical expertise in creating standardized data exchanges in an acceptable format. This includes, but is not limited to the following:

- Chair – Immediate Office of the Assistant Secretary (in accordance with the ACF Strategic Initiatives Plan).
- Co-Chair – On a rotational basis every six months, one from either the OCSE or Children’s Bureau (CB).
- Co-Chair – State or local agency representative from a jurisdiction that has successfully used NIEM or other data standards for a human services project.
- At least three (3) other ACF agency representatives from Family Assistance, Developmental Disabilities, and Administration for Native Americans, Head Start, Child Care and/or others).
- At least one (1) tribal representative.
- One (1) representative from a state actively involved with ACA enterprise solutions involving collaboration with human services programs.
- One (1) representative from a state actively involved with Child Support/Child Welfare (IV-D/IV-E) data sharing projects.
- One (1) additional OCSE representatives involved in on-going data sharing projects including, but not limited to, Federal Parent Locator Services (FPLS), Query Interstate Cases for Kids (QUICK), FPLS SSP, NIEM (data standards).
- One (1) additional children’s bureau representatives involved in on-going data sharing projects (Title IV-E/IV-D data sharing, NIEM, data standards).
- One (1) representative each from CMS and from Food and Nutrition Service (FNS) and SNAP.

NIEM HS Domain Steward Manager

The ACF Assistant Secretary shall appoint the Domain Steward Manager (DSM) who will take primary responsibility for advising and supporting the Domain, the Sponsor, NIEM PMO, and the NIEM Business Architecture Committee (NBAC) on business and technical issues of the NIEM HS Domain.

NIEM HS Domain Governance Group

A standing subcommittee, the NIEM HS Governance Group, made up of human service experts appointed to serve by membership agencies representing the various disciplines in the human services field, will provide subject matter expertise and assistance to further the NIEM standard within the human services sector. The members of the sub-committee will consist of government practitioners at the federal, state, local, and tribal level to recommend domain vision, mission, and goals; monitor progress toward goals; and act on recommendations from the other two domain sub-committees. The appointed candidates will serve as representatives of their various disciplines.

Business and Technology Team

Business and Technology will spearhead the review and creation of NIEM IEPDs and other artifacts and will compile its recommendations for the Steering and Governance Committees. It supports the Domain Governance Group with business and technical expertise related to the human service sector and the NIEM data exchange model as appropriate and to manage the lifecycle of IEPD's once they are approved.

Outreach and Communications Team

Outreach and Communications (O&C) will undertake an internal and external campaign to increase knowledge and understanding of NIEM within the human services community.

Work Groups, Tiger Teams, and Ad Hoc Committees

The HS Domain Governance Group, with approval of the DSM, may establish Tiger Teams to carry out specific tasks. Key stakeholders, practitioners, advisors, and subject matter experts may serve as members of these subcommittees or teams. These subcommittees or teams will be led by a chairperson selected by the HS DSM.

The roles and responsibilities of the various governance committees and groups are summarized in Appendix A-1-6.

3.2.2.4 NIEM-UML

NIEM-UML is the new UML modeling standard in progress for NIEM from the OMG and the NIEM-PMO. NIEM-UML provides for modeling NIEM at a more business-friendly logical level using familiar UML notations and model interchange standards of the OMG. Based on NIEM-UML models, IEPD's and domain updates can be produced or reverse-engineered using model driven architecture automation, thus reducing the complexity and learning curve which are required to produce exchange specifications.

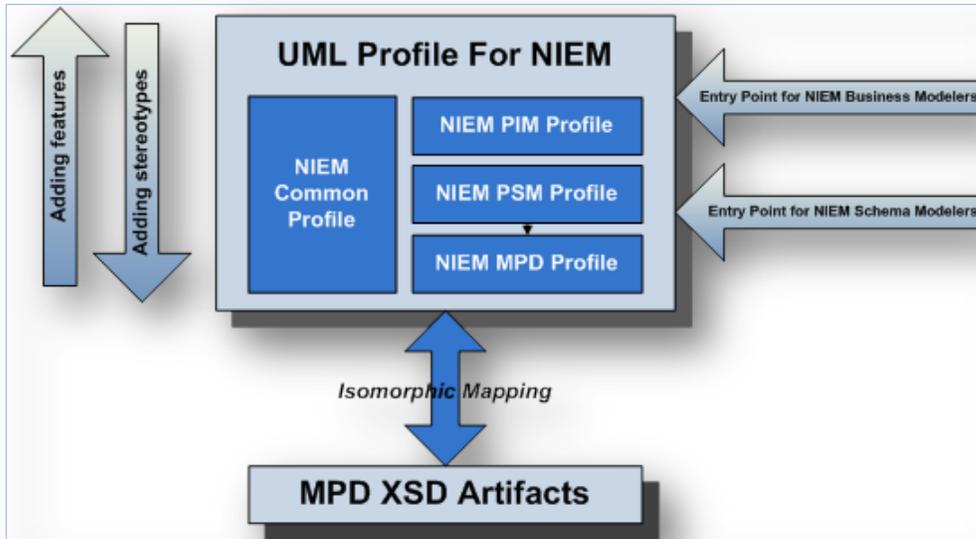


Figure 7: NIEM-UML: PIM & PSM Perspectives

When modeling information exchanges, there are two distinct sets of requirements that lead to two approaches to modeling. The first set of requirements represents the business requirements of an organization. This set is relatively constant and consistent over time and entails modeling the capabilities the organization has, the processes the organization employs and the information the organization leverages. The second set is related to the technical implementation of an organization’s capabilities, processes and information and varies as platforms and technologies change. These approaches are defined by MDA as the Platform Independent Model (PIM) and the Platform Specific Model (PSM) approaches, respectively. The “platform” for NIEM is considered to be XML Schema structured according to the NIEM naming and design rules (NDR) for XML Schema. See Figure 7 above.

The two distinct sets of requirements lead to two different approaches to modeling. The PIM is mainly a business modeling approach while the PSM is mainly a technical modeling approach. In practice, it is important to be able to model an information exchange leveraging both the business and the technical modeling approaches. Furthermore it is critical to have an active communication and effective collaboration between business and technical modelers to assure that the model represents the business requirements correctly and implements them effectively within the means of the current platform and technology. The structure of the NIEM-UML Profile is designed to meet the requirements of the two modeling communities described above and to allow for communication and collaboration between them. NIEM-UML also contains transforms that allow a PIM to automatically produce a PSM (using standard MDA tooling) while allowing the modeler to augment the PIM with PSM considerations as required.

The NIEM-UML has several approaches to data exchanges:

- XML–XSD schemas
- Simple Object Access Protocol (SOAP)
- Web Services

XML is a platform independent language and allows different platforms to talk to each other seamlessly regardless of the difference in platforms. The systems have data stored in various platforms like relational databases, mainframes, IMS. The options would be to either use a Commercial Off the Shelf (COTS) product that can be customized to extract data from all these sources and generate xml files to send to NIEM or to build reusable web services (in–house) that can extract data from all these sources and output it to an XSD-schema mapping the NIEM-UML specifications of the CORE and Domain specific attributes.

3.2.2.4.1 Components of NIEM-UML Specification

The component parts of the NIEM-UML specification are intended to be used together with tools to make it easy to model NIEM in UML and produce valid NIEM platform specifications. The diagram above shows the relationships between the elements of the NIEM-UML specification, a user’s model and the resulting MPD, e.g. an IEPD. It is important to note that the MDA based structure and the separation of concerns between the PIM and PSM part of the NIEM-UML specification allows for representation of NIEM under a different platform if required in the future or to support integration of NIEM into legacy systems. Figure 8 below shows the components of NIEM-UML specification.

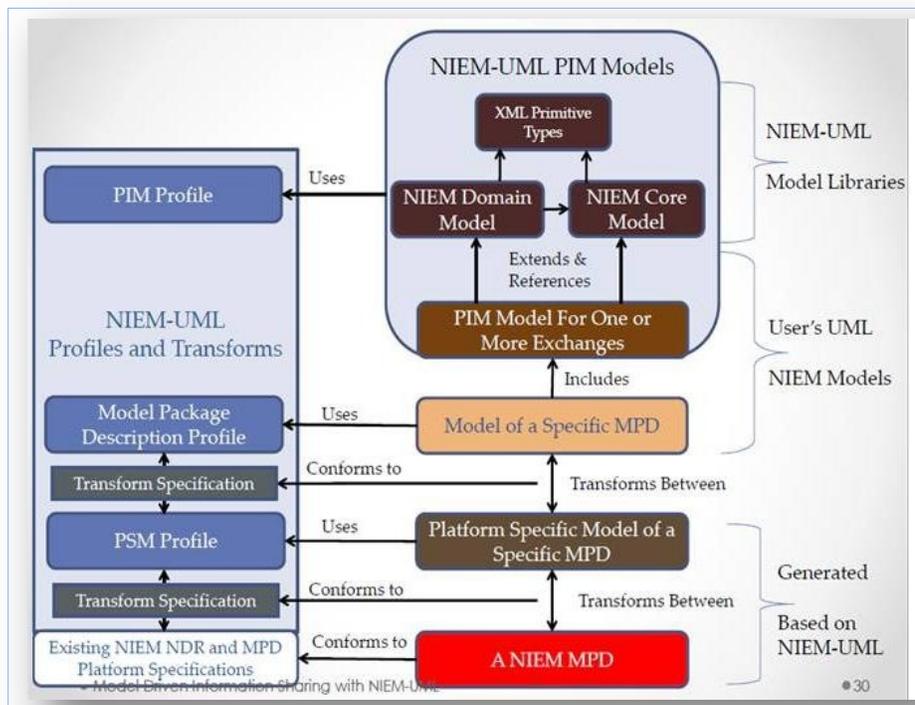


Figure 8: Components of NIEM-UML Specification

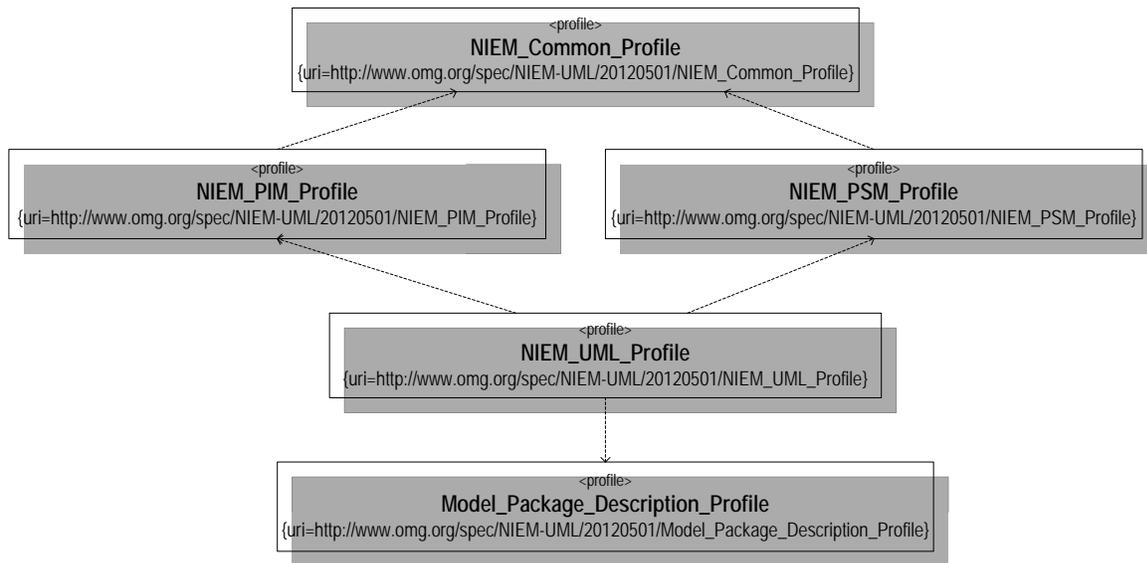


Figure 9: NIEM-UML Profiles

The NIEM PIM Profile and the NIEM PSM Profile, as shown in Figure 9, both import the NIEM Common Profile, which contains the core stereotypes used to represent NIEM structures in UML. For convenience, an overall NIEM-UML Profile is also included, which imports the NIEM PIM, NIEM PSM and MPD Profiles. Applying the single NIEM-UML Profile is therefore equivalent to individually applying all three of the imported profiles.

3.2.3 Medicaid Information Technology Architecture (MITA)

NHSIA is an extension of MITA framework and includes Human Services. MITA uses HL7 for interoperability between messages. NHSIA shares eligibility determination process with CMS out in the states.

3.2.3.1 MITA Framework – Information Architecture (IA)

The MITA Information Architecture describes a logical architecture for the Medicaid enterprise. It provides a description of the information strategy, architecture, and data. MITA IA Components are:

- Data Management Strategy
- Conceptual Data Model
- Logical Data Model
- Data Standards

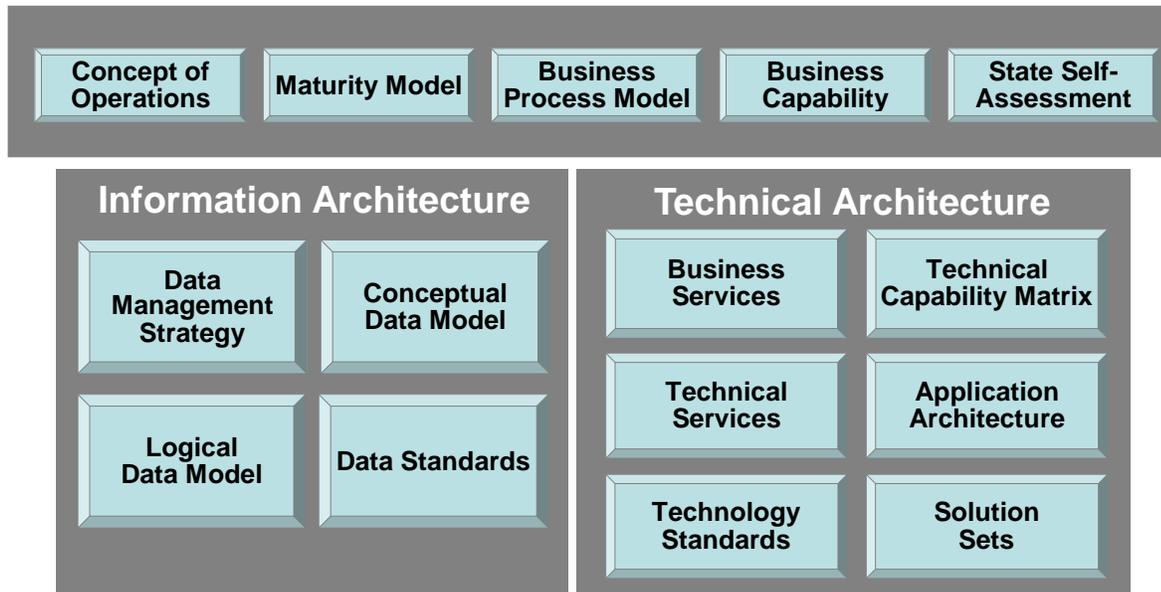


Figure 10: MITA Framework

3.2.3.2 Data Management Strategy

Key components of Data Management Strategy are:

- Data Governance
- Data Architecture
- Data-sharing Architecture

3.2.3.3 MITA Governance Structure

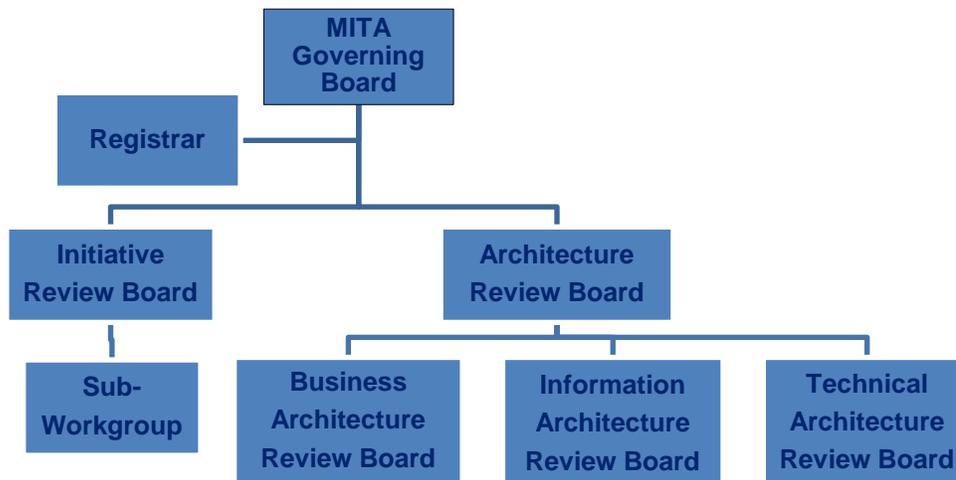


Figure 11: MITA Governance Structure

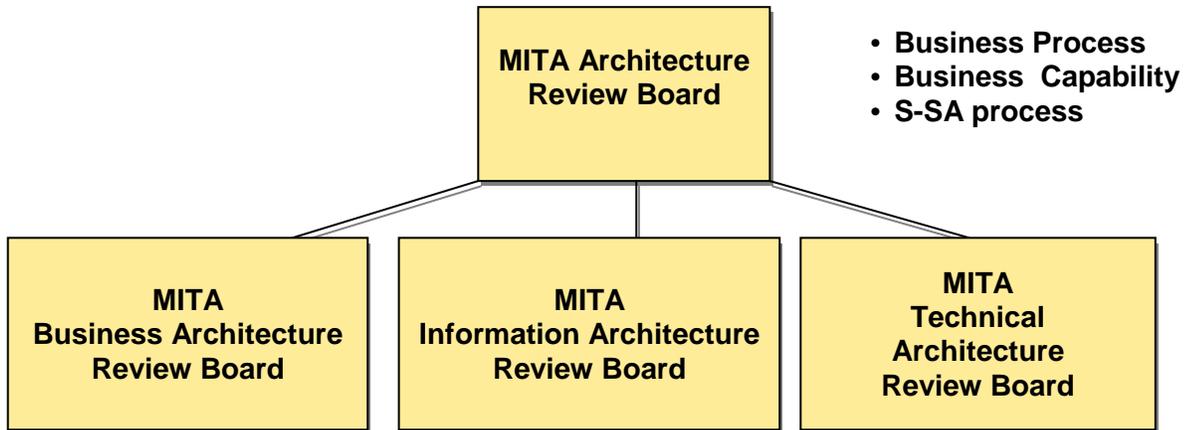


Figure 12: MITA Framework

3.2.3.4 IA Data Architecture

The MITA Information Architecture (IA) provides a conceptual and logical view of all of the data commonly used throughout a Medicaid Enterprise. It describes the integrated information requirements of the Medicaid Enterprise using general data objects and relationships. The architecture is the primary tool for strategic planning, communicating information requirements throughout the organization, implementing integrated systems, and providing an integrated information strategy.

The Medicaid Enterprise data model layer is the pivotal layer of the IA, as it connects reusable business concepts to application-level views of enterprise data through generalized content. Conceptual and logical design of individual processes and services builds the data model layer incrementally. Both the CDM and the Logical Data Model (LDM) are key components to fleshing out the entire data architecture.

States use the LDM to build Logical Application data models including state-specific adaptations and extensions to provide application-specific details. Architects and designers build application data models at both the logical and physical abstraction levels and reuse data objects defined at the enterprise level. This ensures that application models have common keys, attributes, and definitions throughout the enterprise data architecture. A single entity in the data model exists in multiple application-specific models with attribute and code set variations based on business need (i.e., rules) or as subtypes of more generic enterprise entities. A single entity in the MITA data model supports data consistency and reuse.

The IA provides states with guidance on selecting a data management strategy that meets national standards for data sharing and interoperability. It also enables states to use common strategies (e.g. data hubs) when designing Medicaid information solutions.

States, CMS, vendors, legislators, and others will use the architecture's components to plan for improvements in the State Medicaid Enterprise, both in the delivery of services

(i.e., to providers, beneficiaries, and citizens), and in its internal operations and exchanges of information with other external parties.

3.2.3.5 Data-Sharing Architecture

Data-sharing architecture describes technology considerations for the State Medicaid Enterprise to participate in information-sharing communities. Based on business requirements, the MITA team (with support from state and vendor supported workgroups) defines the data and information exchange formats. The Medicaid community defines or adopts standard data definitions and data-sharing schemas. It is a goal that a centralized dictionary and directory maintains this information for general use. Each State Medicaid Agency (SMA) is responsible for knowing and understanding its environment (e.g., data, applications, and infrastructure) in order to map its data to information-sharing requirements. The data-sharing architecture also addresses the conceptual and logical mechanisms used for data sharing (i.e., data hubs, repositories, and registries). The data-sharing architecture also addresses data semantics, data harmonization strategies, shared-data ownership, S&P implications of shared data, and the quality of shared data. State solutions should promote sharing, leverage, and reuse of Medicaid technologies and systems within and among states, thereby reducing costs.

3.2.3.6 Data Standards

Completing the IA requires the definition of data standards. Data standards describe objects, features, or items collected, automated, or affected by the business processes of a State Medicaid Enterprise. A data management strategy identifies the patterns in the Medicaid Enterprise for the exchange and sharing of Medicaid information. Identifying the patterns allows the development of optimal data governance procedures, data architecture and data-sharing architecture for the Medicaid Enterprise.

The Scope of Data Standard as defined by MITA:

- MITA will use data standards produced by designated standard maintenance organizations (DSMOs) or Standard Developing/Development Organization (SDO) whenever available.
- If such standards are not available, MITA will facilitate the development of specific data standards and submit them to a DSMO/SDO for adoption whenever possible.
- Because data standards are quite dynamic, a periodic review of the available data standards and versions is needed to keep the MITA data standards current
- The MITA data standards will be extended to be compatible with Electronic Health Record (EHR) once they are defined.
- MITA data standards will not map to information for State-specific data and messages.
- Data standards associated with the physical data model, databases, and data files will not be part of MITA.

Existing MITA Data Standards represents agreements on the format and description of the shared data used by the Medicaid enterprise. There are two major categories, structure data standards and vocabulary data standards which address data aspects such as:

- Data element names
- Definitions
- Data types
- Formatting rules

As stated above, standards are dynamic, and an associated MITA Data Standards Development Process should be used for both review and development. The process is described below:

- Identify standards already in use by current State Medicaid systems
- Align data standards with data model entities/attributes and messages
- Only develop new standards when no alternatives exist. Data standards will typically be adopted in the following order of priorities:
 - ✓ International standards
 - ✓ National standards
 - ✓ Industry/healthcare standards
 - ✓ MITA or State developed standards
 - ✓ Adopt a minimum standard that is usable by the maximum number of State Medicaid enterprises
 - ✓ Allow versioning and allocate the standard to MITA maturity levels
 - ✓ Submit to the MITA governance process
 - ✓ Maintain on the MITA repository

For reference, the following list of key Standard Development and Maintenance Organizations is provided:

- American Dental Association (ADA)
- Accredited Standards Committee (ASC) X12N – Insurance Subcommittee
- Dental Content Committee of the ADA (DeCC) (DCC)
- Health Level 7 (HL7)
- National Council for Prescription Drug Programs (NCPDP)
- National Committee on Vital and Health Statistics (NCVHS)
- National Institute of Standards and Technology (NIST)
- National Uniform Billing Committee (NUBC)
- National Uniform Claim Committee (NUCC)

In Figure 13 shown below, MITA is aligned with Federal Enterprise Architecture (FEA).

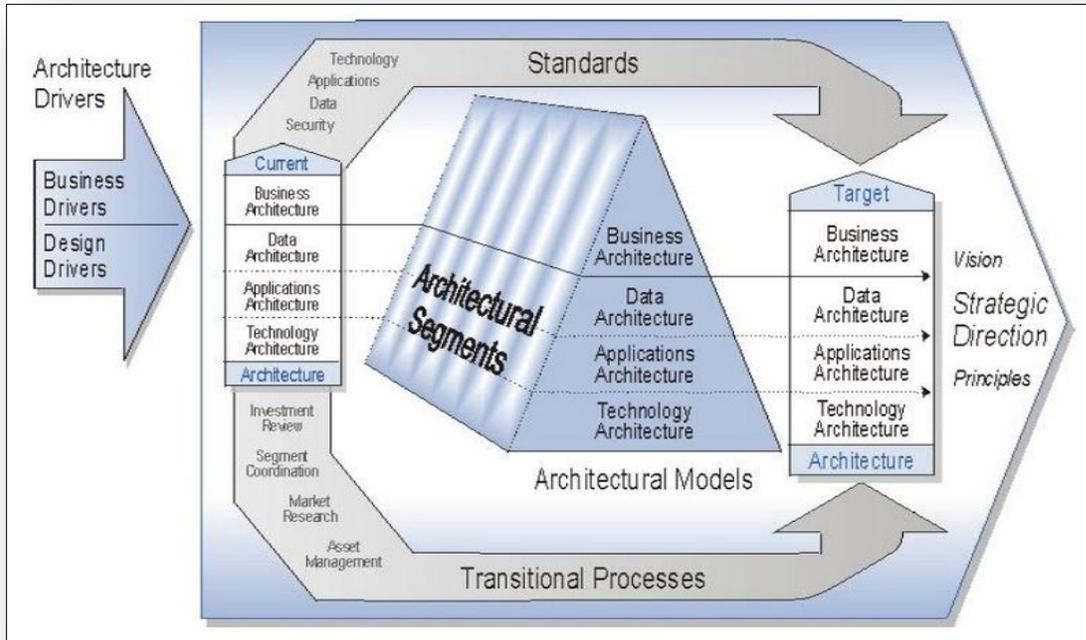


Figure 13: Federal Enterprise Architecture (FEA)

NHSIA and MITA are closely aligned. NHSIA satisfies the seven conditions of MITA.

Table 5: MITA Conditions and Standards/NHSIA Features

MITA Seven Conditions and Standards	Representative NHSIA Features
Modular systems development	SOA; reusable components; business rules separate from systems
Align with MITA	NHSIA business viewpoint adapted from MITA; SOA
Use industry standards	MITA; NIEM; GRA; GFIPM
Share and reuse technology	Shared services, hubs, & HIX/Medicaid components; integrated eligibility
Deliver business results	NHSIA PRM; Business viewpoint drives technology; automated processes
Performance reporting	NHSIA PRM; cross-program performance information repositories (PIRs)
Interoperable across health & human services community	NIEM info exchanges; verification services; shared enrollment data

3.2.3.7 Data Sharing – Master Data Management (MDM)

Spanning data governance, data architecture and data sharing, MDM addresses the goal of delivering a single, unified and accurate view of enterprise information. MDM integrates information from various data sources into one master record. This master data is then used to feed information back to the applications, creating a consistent view of information across the enterprise.

3.2.4 Master Data Management (MDM)

The Data Architecture for interoperability will create a MDM System that will be the storage and retrieval area of master data.

Maintaining detailed master data records remains a particularly important aspect of any Data Governance practice, especially concerning regulatory compliance issues.

When we deploy MDM solutions as a foundation for and in combination with SOA, all the potential business value from the data quality improvements are realized as this quality data finds its way to every application and business process that needs it. And all the potential improvements in flexibility from the SOA implementation are realized as they operate across application boundaries without faults due to data errors.

SOA enables business functionality as a service. However, it does not guarantee quality of the data on which it's operating. That's a serious gap, which is filled by including MDM in a service-oriented architecture. True business value is realized as services start leveraging the high quality data in the MDM hub and the services which surround it.

MDM abstracts the governance of data by consolidating it into a central data model; conducting all data cleansing, augmentation, cleansing, and standardization; and creating a 'gold standard' source. These data management functions are centralized in the data hub and are hidden from the consumers of the cleansed data. Maximize the value of these services by consuming them from other applications that need to perform data quality processing external to the data hub.

The main goals for MDM:

- Interoperability
- Single point for data sharing/usage/reuse and for reference purposes
- Single point for data maintenance
- Low operating/maintenance costs
- Less error prone
- Easier to manage master data

The seven building blocks of success for MDM are (Source: Gartner):

- MDM Vision
- MDM Strategy
- MDM Governance
- MDM Organization
- MDM Processes
- MDM Technology Infrastructure
- MDM Metrics

3.2.4.1 IBM's Reference Architecture (RA)

The IBM's MDM Reference Architecture is a reference architecture that supports implementing the multiple methods of use (collaborative, operational, and analytical) for MDM and multiple implementation styles (registry, coexistence, transaction style). It enables the ability to design business solutions incorporating MDM capabilities.

An MDM solution derived from the MDM RA enables an enterprise to govern, maintain, use, and analyze complete, contextual, and accurate master data for all stakeholders, users, and applications, across and beyond the enterprise.

The different methods of use of MDM include:

- **Collaborative:** Collaboration means that multiple users, usually in different roles, participate in the same process on a master data entity. A typical example would be the collaborative authoring of product master data where item specialists, brand category managers, pricing specialists and translators collaborate to author the definition of a new product. Key requirements of collaborative method of use are workflow support with check-in/check-out functions, support for relationships, and product hierarchy management. From a security perspective, attribute-level granularity of authorization privileges across all functions such as workflow, relationship and hierarchy management must be available for implementation.
- **Operational:** This method of use is important when an MDM System has to function as an Online Transaction Processing (OLTP) server. Typically, a large number of applications and users require quick access to master data to retrieve and change master data through MDM services invoked by business processes such as "New Account Opening". The MDM services are often used in the context of an SOA and need to be accessible through a variety of interfaces. MDM Systems supporting this method of use might have the need to support several hundred transactions per second on millions of master data records.
- **Analytical:** This method could either be identity focused master data focused or integration-focused.
 - **Identity analytics:** This sub-type is usually encountered when there is a need to determine or verify an identity and discover hidden relationships.
 - **Analytics on master data:** Here, an MDM System needs to answer questions such as "How many new customers did I receive over the last day?" or "How many customers changed their address in the last week?"
 - **Analytics integration with data warehouses:** First, an MDM System provides master data to the data warehouse for accuracy improvements in the data warehouse environment. In a second step in this sub-type of the analytical method of use, insight gained in the data warehouse is made actionable by feeding it back to the MDM System for use in the IT landscape. An example of this analytical method of use is to persist the computed customer profitability metrics and customer potential metrics in the MDM System, so that, from there, this insight can be leveraged in all front and back office systems.

There are different **implementation styles** to accommodate the variety of requirements. Often an enterprise starts with one style and evolves their implementation to continue driving business value to the organization. The three styles are:

- **Registry style:** This style provides a read-only view to master data for downstream systems which need to read but not modify master data. This implementation style is useful to remove duplicates and provide (in many cases federated) a consistent access path to master data. The data in the MDM System is often only a thin slice of all the master data attributes which are required to enforce uniqueness and cross-reference information to the application system that holds the complete master data record. In this scenario, all attributes of the master data attributes remain with low quality without harmonization in the application systems except for the attributes persisted in the MDM System. Thus, the master data is neither consistent nor complete regarding all attributes in the MDM System. The advantage of this style is that it is usually quick to deploy and with lower cost compared to the other styles. Also, there is less intrusion into the application systems providing read-only views to all master data records in the IT landscape.
- **Coexistence style:** This style fully materializes all master data attributes in the MDM System. Authoring of master data can happen in the MDM System as well as in the application systems. From a completeness perspective, all attributes are there. However, from a consistency perspective, only **convergent consistency** is given. The reason for this is that there is a delay in the synchronization of updates to master data in the application systems distributed to the MDM System. This means, consistency is pending. The smaller the window of propagation, the more this implementation style moves towards absolute consistency. The cost of deploying this style is higher because all attributes of the master data model need to be harmonized and cleansed before loaded into the MDM System which makes the master data integration phase more costly. Also, the synchronization between the MDM Systems and application systems changing master data is not free. However, there are multiple benefits of this approach that are not possible with the Registry Style implementation: The master data quality is significantly improved. The access is usually quicker because there is no need for federation anymore. Workflows for collaborative authoring of master data can be deployed much easier. Reporting on master data is easier – now all master data attributes are in a single place.
- **Transaction style:** With this style, master data is consistent, accurate and complete at all times. The key difference to the Coexistence Style is that both read and write operations on master data are now done through the MDM System. Achieving this means that all applications with the need to change master data invoke the MDM services offered by the MDM System to do so. As a result, **absolute consistency** on master data is achieved because propagation of changed master data causing delay no longer exists. Deploying an MDM solution with this style might require deep intrusion into the application systems intercepting business transactions in such a way that they interact with the MDM System for master data changes or the deployment of global transaction mechanism such as a two-phase commit infrastructure.

Figure 14 shows the IBM MDM Logical System Architecture.

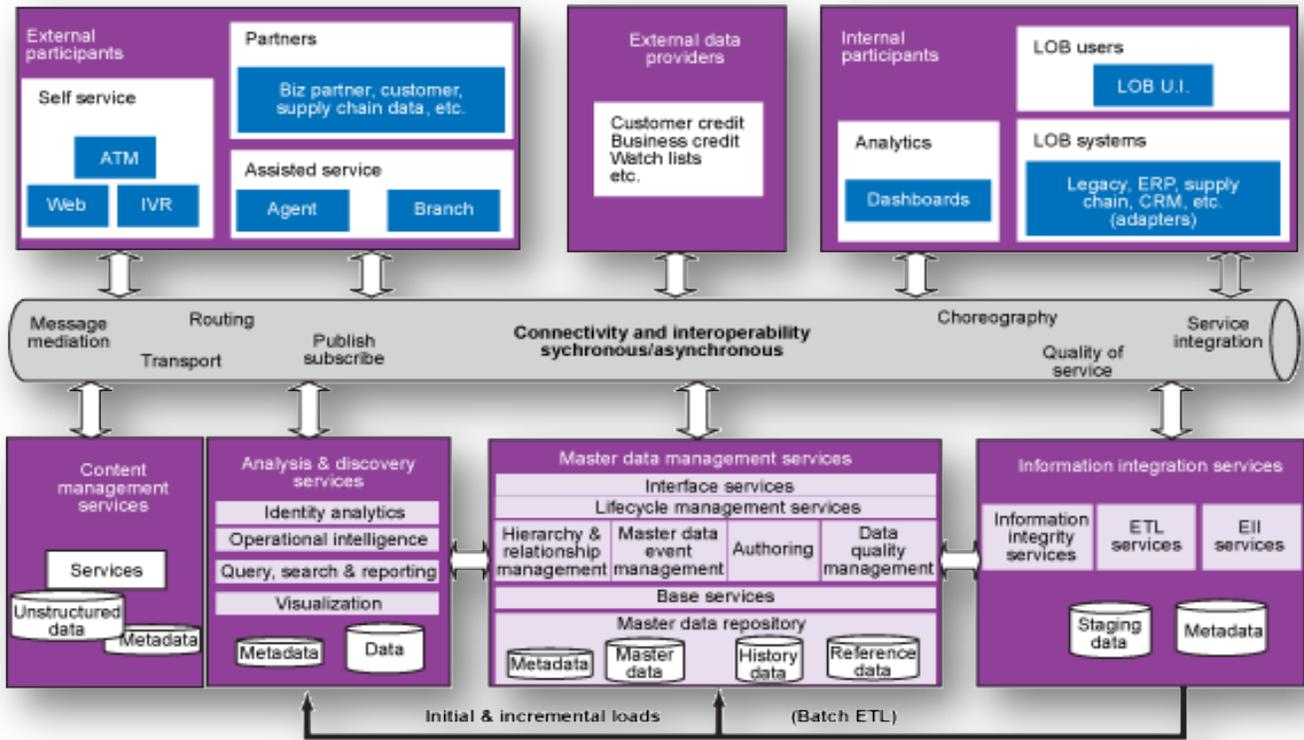


Figure 14: IBM MDM Logical System Architecture

Based on the architecture that we choose as reference architecture, tools are available in the market that would implement the MDM architecture.

As an example below in Figure 15, the RA is mapped to IBM Tools:

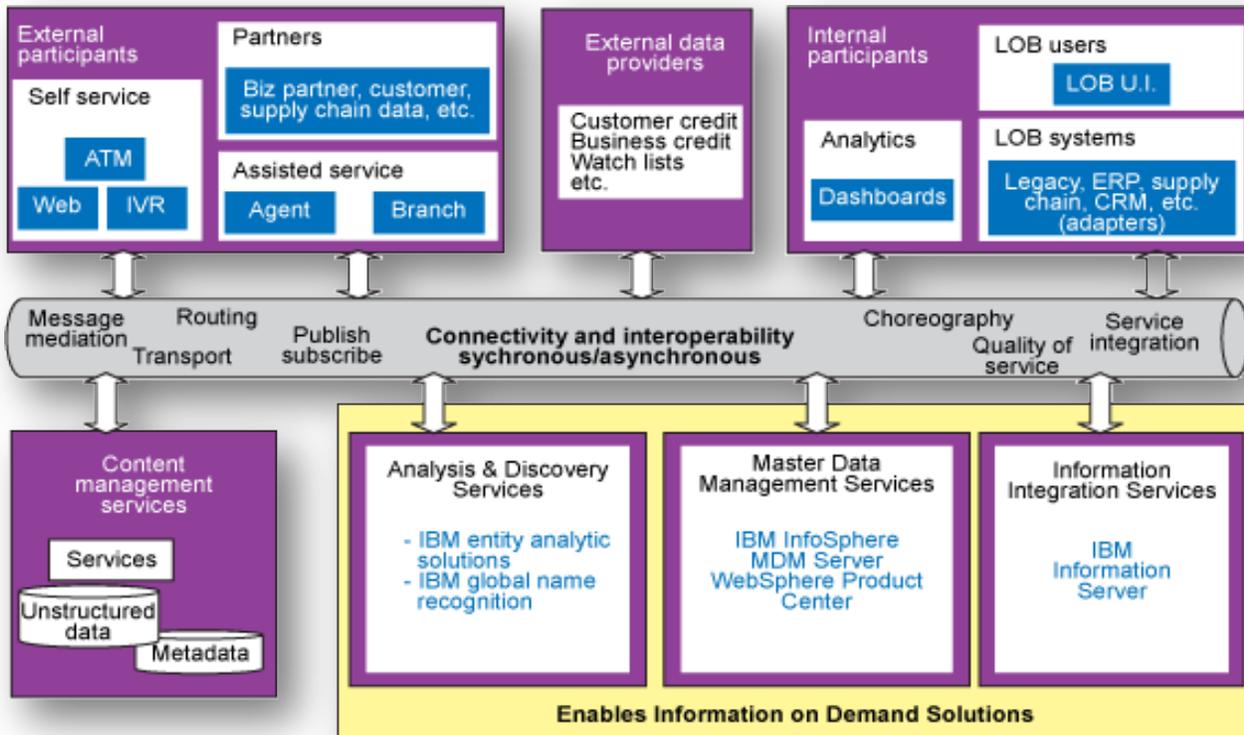


Figure 15: Example Mapping RA to IBM Tools

3.2.4.2 Data Offered by the MDM Hub

Data services allow the consuming application to access and manipulate hub data from a service layer as a supported data source. Layering data services on the MDM hub hides the implementation of federated queries that gather the data requested by the consumer.

3.2.4.3 SOA, MDM, and Middleware

SOA, integration middleware ESB, and MDM together can manage the detection of data changes in the source applications and propagate them from the source applications to the MDM – or from the MDM back to the consumers. With the addition of Business Process Execution Language (BPEL) and a business rules engine, a data change detected in a source can be captured due to the data quality business rules to be executed on the data, and place the data back on the ESB to be consumed.

3.2.4.4 Software AG Process–Driven Master Data Management

Process-driven MDM attacks master data problems from a business perspective. It seeks business objectives and definitions of success. Processes for Process-Driven Master Data Management:

- Identify processes impacted by poor master data
- Describe data quality (DQ) issues impacting process performance
- Quantify key performance indicators (KPIs) that show the effect of poor master data on process performance
- Identify which master and reference data is used by processes (for example, tire SKU#)
- Describe how data is used by processes: created, enhanced, modified, deleted etc.

The following are the prevalent styles for MDM implementation:

- **Consolidation:** Master data is authored (created, updated, deleted) in several transactional systems and consolidated into the MDM Hub as the Golden Record. Matching, merging, and cleansing of data are done within the MDM Hub. Master data is not entered directly in the MDM Hub, and it is not written back to the transactional systems.
- **Centralized:** Master data is authored and governed centrally within the MDM Hub and deployed to other systems in your landscape.
- **Registry:** In this style, data authoring is done within transactional systems. Master data isn't moved to the MDM Hub; instead, the hub stores pointers to the master data which continue to remain in the transactional systems, in order to identify the record in the transactional systems.
- **Hybrid:** Master data authoring can be done in the transactional systems as well as in the MDM Hub. Sanitized master data can be written back to transactional systems.
- **Coexistence:** Master data is entered in transactional systems only. After utilizing an MDM Hub as a kind of Data Quality Service, sanitized master data can be written back to the original transactional system as well as being distributed to other transactional systems. This integration style is usually established when a centralized approach isn't feasible because historically several data hubs have been established.
- **Central Deployment Hub:** In this scenario, master data from a source is taken as it is (single source of truth, also previously known as Dominant Source). The master data may be enriched and then distributed to various other systems.

3.2.5 Case Studies for eMPI

Option 1 (Case Study A – Identifying a person across agencies)

In the Interoperability Grant Project, we can take an example of identifying a person across the agencies. If the data is not kept up to date and there's duplicate data, process of delivery of data/service to the systems might be delayed. Time spent in going through a process for removing duplicates/cleaning data will degrade the performance of the service and delay the delivery of the service. KPIs for this process could be time spent on cleansing data, time spent on resolving duplicate data, delay in getting results, manual intervention might be necessary).

Matching Criteria for a person for all five participating agencies were studied as an approach on how to most effectively design the MDM hub useable by all participating agencies without giving it a scope so broad that it would be hard to keep focus on our goals. In the current scenario, state mandate does not allow Birth Certificate data to be included in the shared eMPI but might be in a restricted manner in the future pending agency and legal approval.

During the requirements gathering phase of a MDM implementation, the DGO is involved in defining the scope of requirements for data that will be managed in the MDM hub. Several categories need to be considered, including: Entity Types; Ownership and Accountability; Policies, Processes and Standards; Data Integration (Inbound and Outbound); Service Level Agreements; Data Quality; Match and Merge (Survivorship); User Interface and Security; General Maintenance. Requirements, documents of policies/procedures, agreements, data quality, security are being gathered from the participating agencies excluding the Federal and Other State Agencies (State IV Agencies).

The matching criteria for a person for all five participating agencies are given below in Table 6:

Table 6: Matching Criteria

• OKDHS Client Identifier	• Birth Day
• OHCA Client ID	• Birth Year
• SSN	• Gender
• First Name	• Mother Maiden Name
• Last Name	• OKDHS Case Number
• Middle Initial	• OSDH Birth Certificate Number (Internal to OSDH Birth System)
• Birth Month	• OHCA Case Number

The diagram below depicts the role of MDM in SOA Architecture. Since Business Processes still need to be identified for the TO-BE system, we are only giving a generic architecture. It could change based on the specific Business Rules identified for the data exchanges. But even if there could be minor changes, the basic architecture of achieving

interoperability of master data between the agencies could be based off of the diagram below with eMPI focus. This is a **Repository Approach** (centralized) to an MDM.

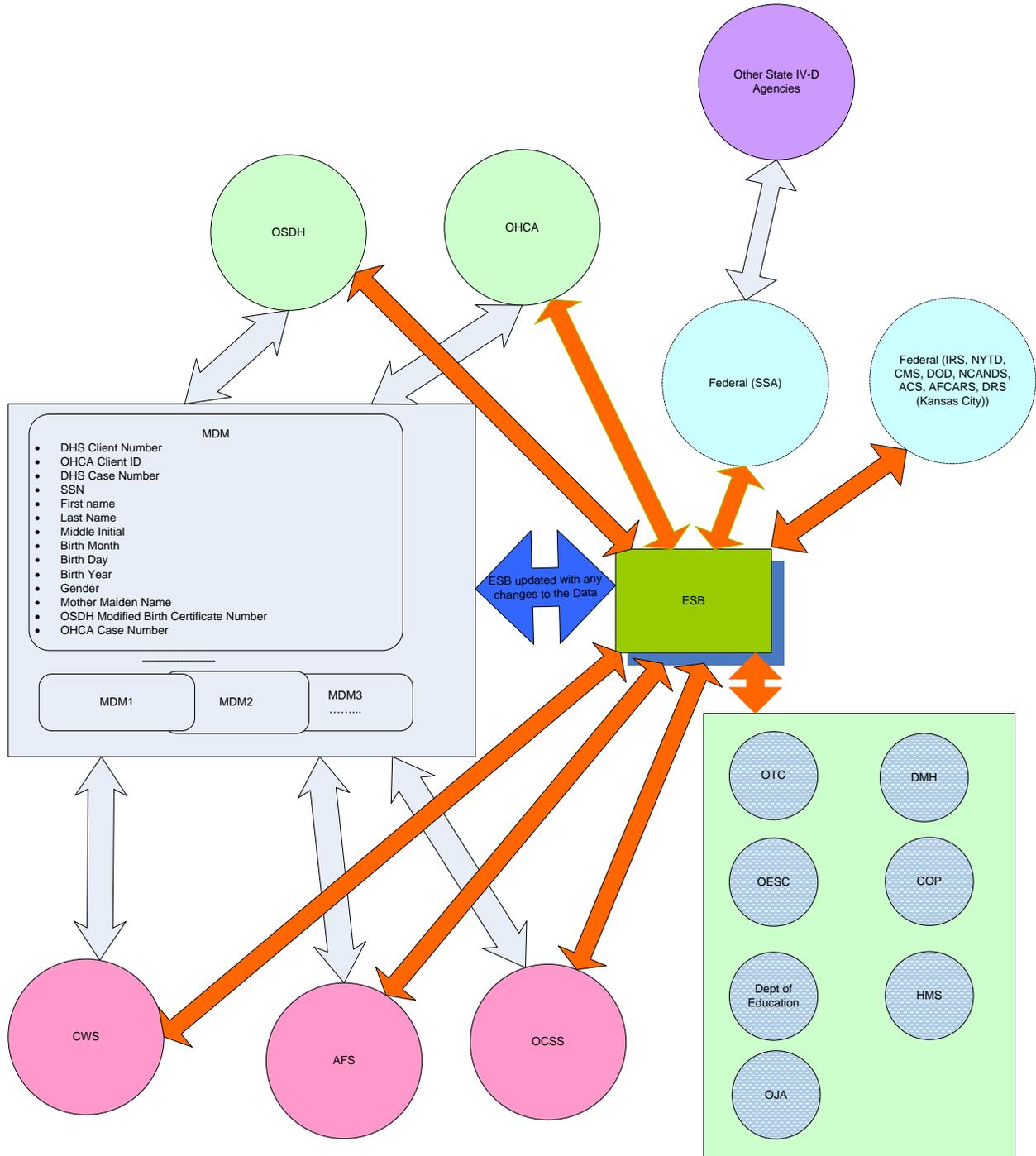


Figure 16: Interoperability using matching criteria with MDM for eMPI

The details of how each system accesses data elements included in the matching criteria is shown in Appendix A-1-7.

Option 2 (Case Study B – Hybrid approach)

Since state mandate does not allow OSDH to share birth information as an eMPI, we could leave the repositories with the agency but still allow other agencies to use the matching criteria for creating an MDM. The MDM would, in this case also have an arbitrary number that maps back to each agencies including OSDH. This is the **Hybrid Approach**.

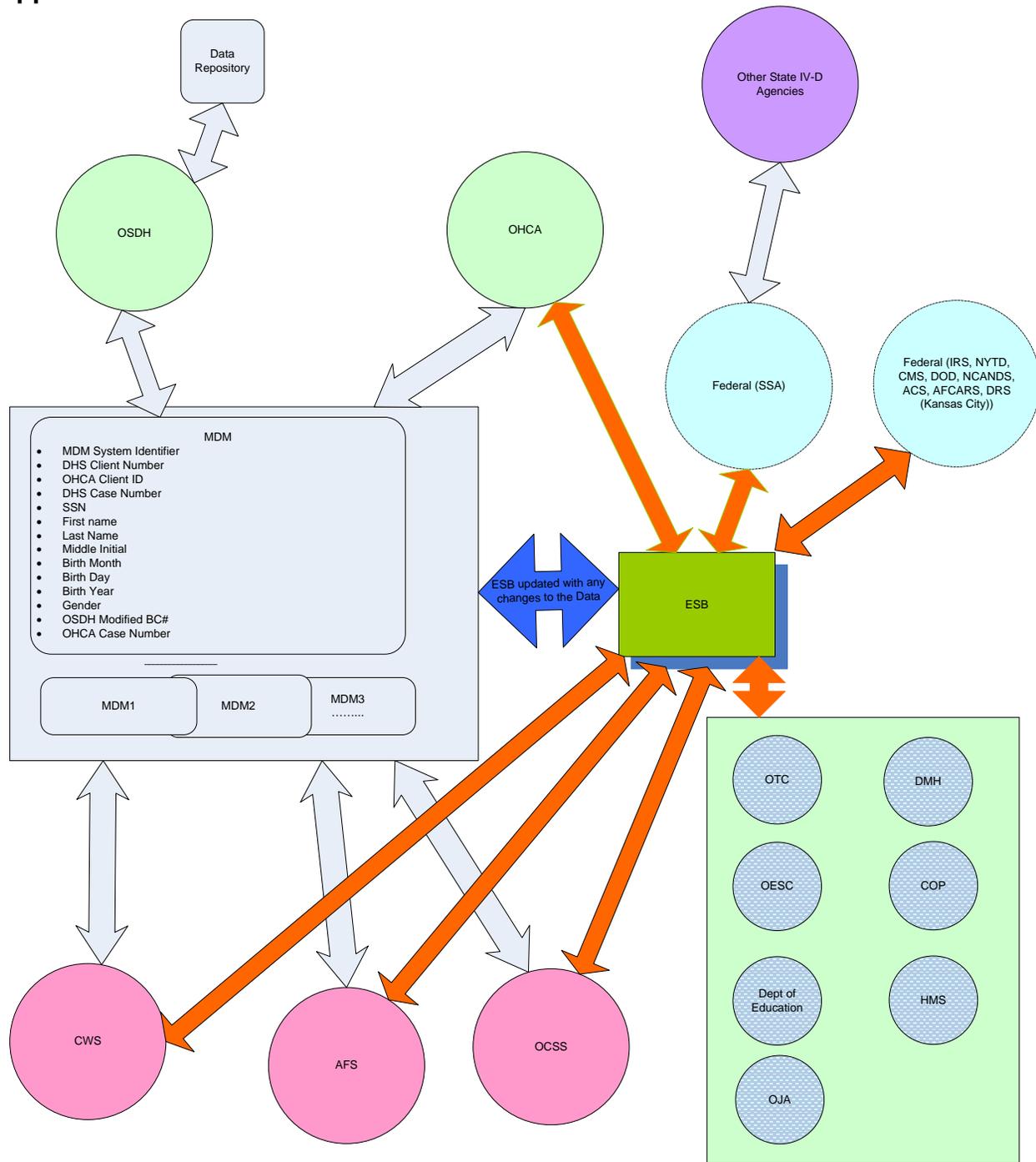


Figure 17: Interoperability using a Hybrid Approach for MDM and eMPI

Option 3 (Case Study C – Using a unique arbitrary number as an eMPI to share across the agencies)

Option 3 was considered as an approach to create an eMPI with an arbitrary number that can be shared across all agencies. It involves creating the MDM hub that contains lists of keys that can be used to find all the related records for a particular master-data item. For example, if there are records for a particular client in the AFS, CWS, OCSS, OSDH and OHCA databases, the MDM hub would contain a mapping of the keys for these records to a common key. This is the **Registry Approach** of creating the MDM, see Figure 18.

We might also consider several other MDMs for storing Client Demographics, Case Management, and Claim Processing etc.

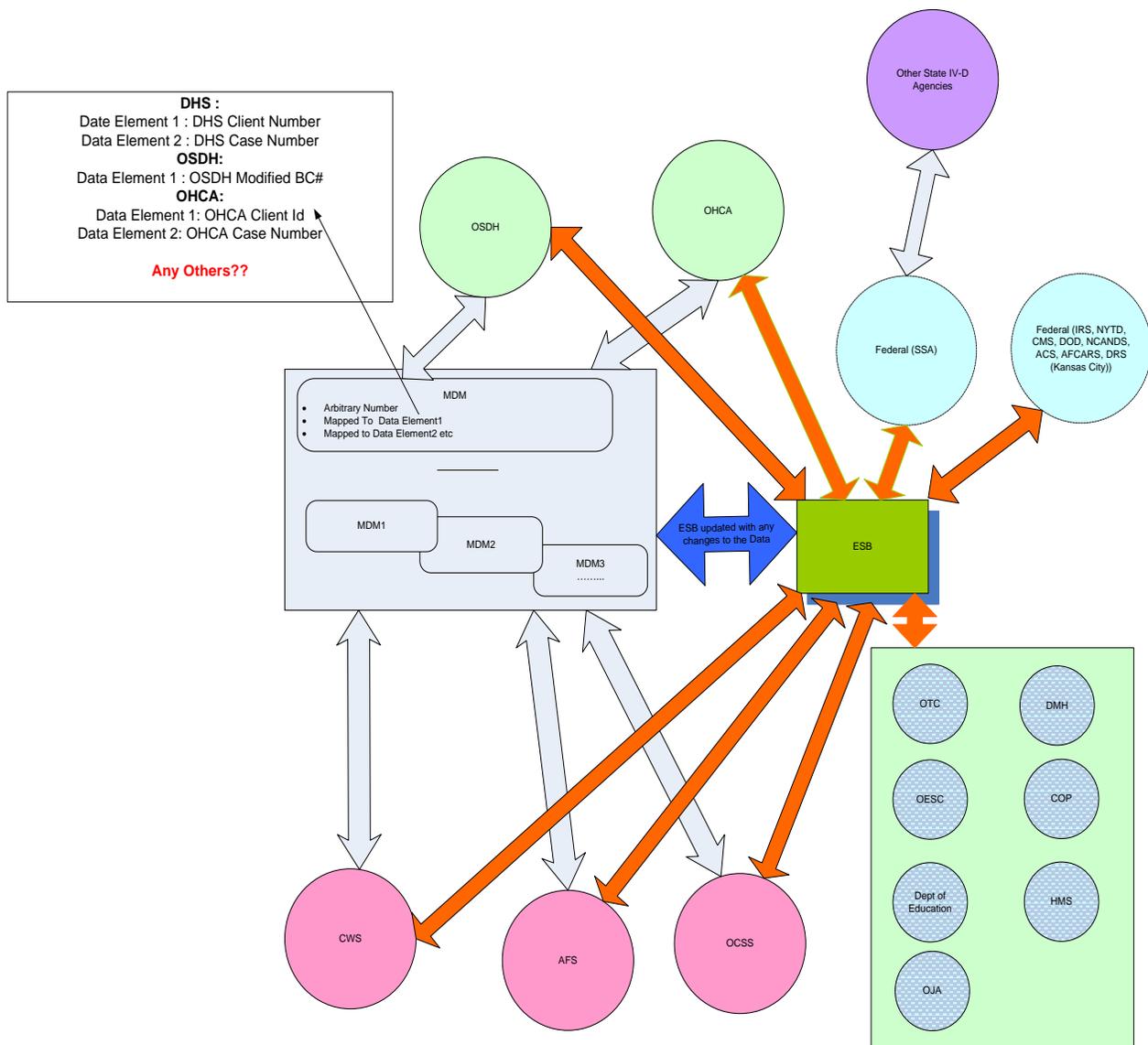


Figure 18: Interoperability using Registry Approach for MDM and eMPI

3.2.6 System Diagram – Data Flows to/from Business Processes

Figure 19 shows the dependency/flow between the business processes and the information exchange processes. Information exchanges can be leveraged using Web Services, reports or ad hoc queries at the application level; Web Services, reports, are, in turn, based upon the Business Processes and Business Requirements. Ad-hoc queries are run based upon the Business needs/requirements.

ESB serves as the model for designing and implementing interaction and communication between Software Applications (e.g. Web Services) in SOA.

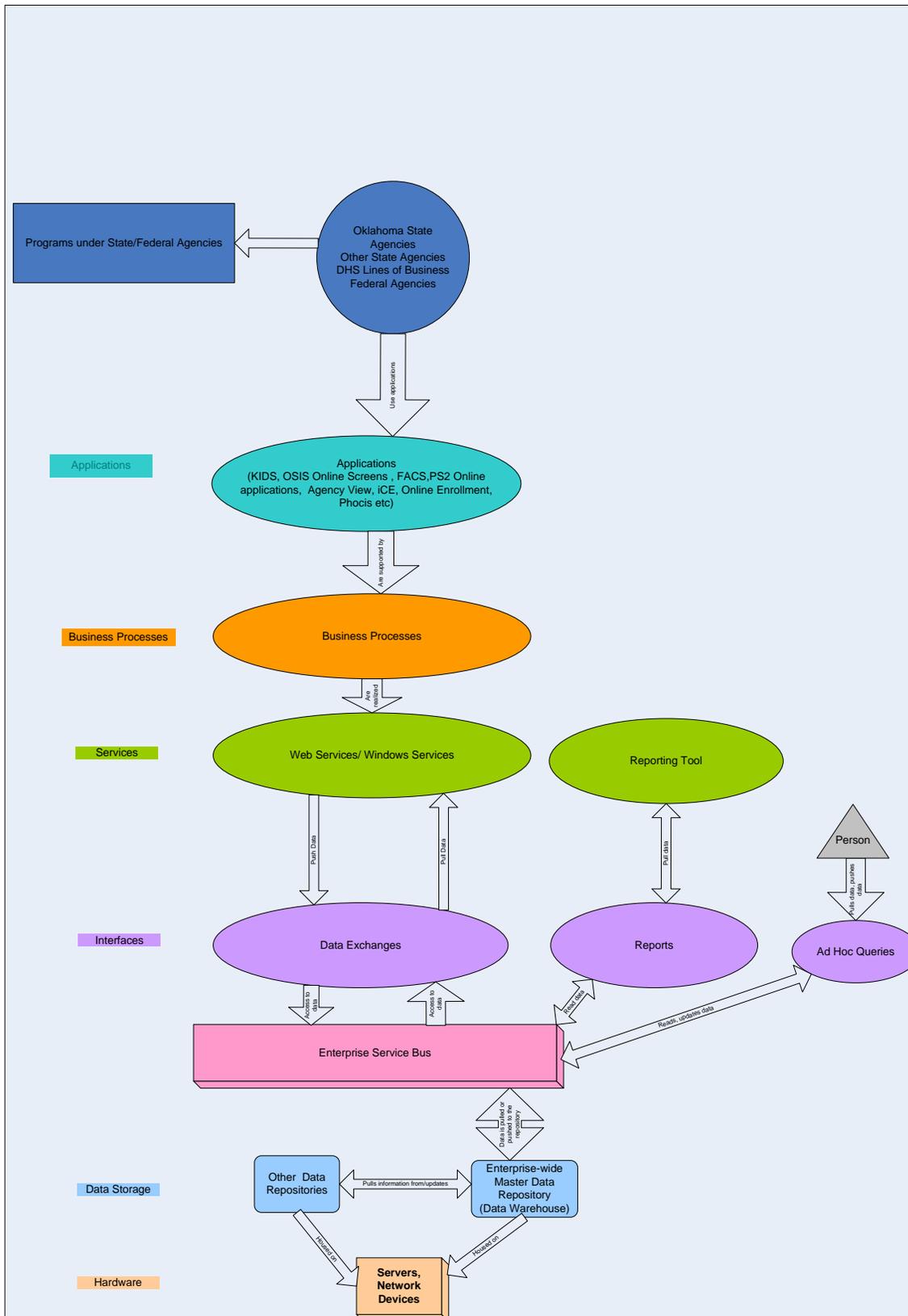


Figure 19: Data Flow Process

3.2.7 Security and Integrity

As applicable, describes how access security will be implemented and how data transmission security will be implemented for interface being defined.

In the AS-IS system, most of the transmission (data exchange) with an outside agency is done via FTP or secure FTP. The data is either saved on the agency's server to be picked up by another agency or data is FTP'd to the server on another agency by FTP/SFTP. Within DHS Lines of Business jobs are being run to transfer a flat file and store it on a server. Some interfaces access the data real time, in this type of transmission there is no FTP, SFTP involved and data is accessed Real-Time via a User Interface. User Interface could be a web based application or a report run on a system or just an online application (not web-based).

For Real-Time applications the access is restricted by the proxies that are created for the database. The application cannot access information if the proxy/password combination is not correct.

SFTP uses a secure channel to exchange data from the 'sender' and the 'receiver'. Thus the sender knows that the recipient is the ultimate destination.

In the TO-BE system since the plan is to make it Service Based, the security should be handled at the service level for exchanging data.

Data Security should be governed by Data Governance board and IT Steering committee. Data Stewards should be involved in creating new Policies and Procedures for the data security of data storage and data exchanges, also making sure that compliance with organization Security Policies and Procedures are always met. Currently we have Security Policies defined at the organizational level for DHS and for exchanges with OHCA and also Federals.

With OHCA, at the project level data security measures are handled through agreements and various processes like change management process.

An interface, completely self-contained, such as movement of data between systems resident in the same computer room, may not have any security requirements. In this case, explanation included of why interface has no security and integrity requirements.

For the TO-BE system, security of content, applications and data need to be taken into consideration. Security can be handled by introducing hardware (communication devices) in certain cases and by having a centralized data store in a secure area from the infrastructure point of view. The firewalls, secure web services, encryption, authentication, authorization, identity management, other secure services will enforce security of the data. Unsecure mechanism of data transfer, such as using email to transfer data, needs to go away. A preliminary vision of security is given in Figure 20.



Figure 20: Security Vision

The federal government has defined a security standard to facilitate interoperability, encourage the use of best practices, and shorten project schedules. This standard is called Global Federated Identity and Privilege Management (GFIPM). Specifically, GFIPM was created to standardize how exchanges secured their environment, focusing on the following:

1. Authentication of users
2. Encryption of data to maintain privacy
3. Authorization based on user attributes and the context of the request

In order to meet these requirements, GFIPM uses the following foundational standards:

1. Web Services Security
2. WS-I Basic Security Profile
3. SAML-based authentication
4. SAML-based attribute assertions
5. XACML-based authorization

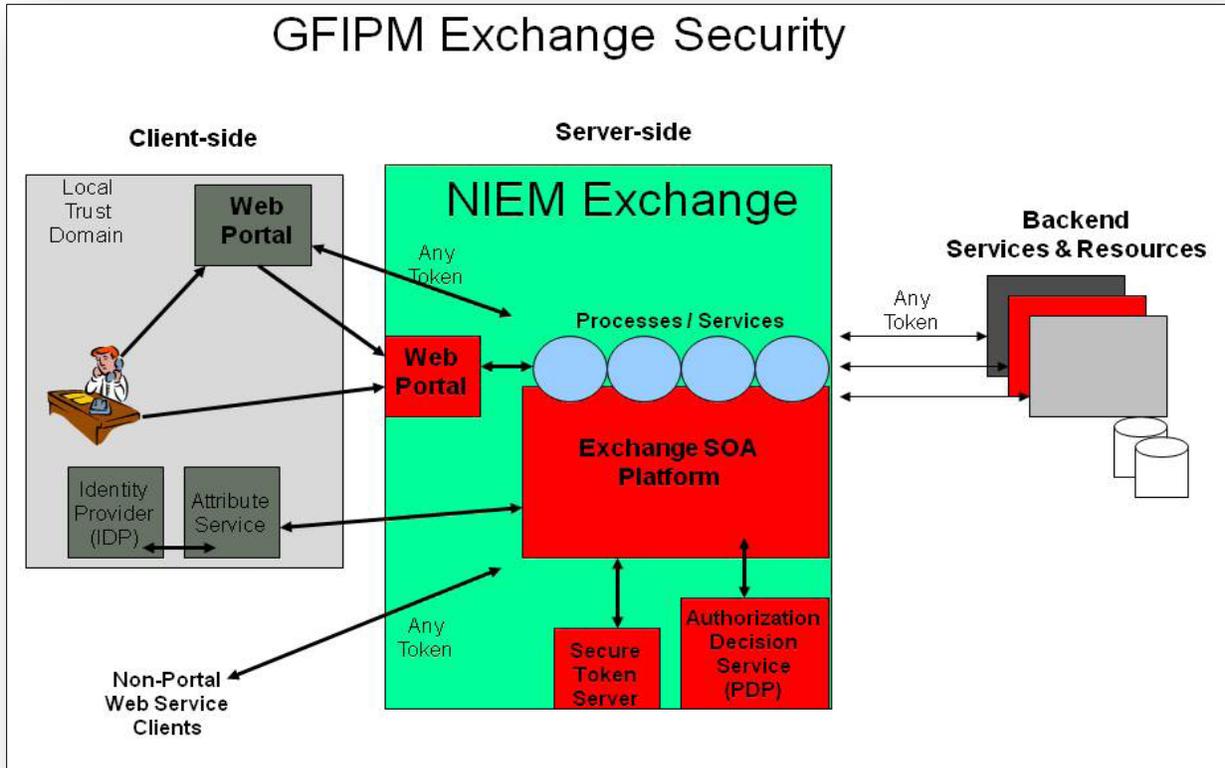


Figure 21: GFIPM Exchange Security

Figure 21 shows the Security Architecture of GFIPM.

One of the challenges in this environment is converting from one set of security credentials (“tokens”) to the GFIPM standard using SAML and supporting GFIPM user attributes. The user credentials need to be captured. One must query an authorization service to determine whether the user should be granted access.

The concepts developed as a part of GFIPM provide a proven approach that NHSIA can follow. The mission of the Global Reference Architecture, the parent of GFIPM, is “to enhance justice and public safety through a service-oriented approach to information sharing.” NHSIA has a similar mission with respect to health and human services. Similar Security architecture can be implemented for NHSIA which will apply to Human Services.

3.2.8 Recommended Approach

1. Assessment/gap analysis of current interfaces. Group the AS-IS interfaces from Appendix A-1-1 to map to NHSIA’s Information exchanges (Appendix A-1-8). This would require a substantial amount of time working with the Stakeholders (work going on with some teams in this aspect). Results from the OKDHS teams are

attached in Appendix A-1-9. These results need to be assessed for collaboration between agencies and to streamline the exchanges.

2. Review NIEM/NHSIA governance. Identify the gap that NIEM HS Governance structure does not cover.
3. Work on the Data Governance for the agencies for data stored within the agencies, and also on the governance of data exchange that NIEM's HS Domain Governance structure does not cover.
4. Work on the best practices for implementing MDM architecture. Consider several approaches and pick up the one that is most cost beneficial and helps achieve interoperability without compromising the performance and data quality issues. An approach that would allow sharing of the data keeping integrity intact, and also allow privacy/security at a high level.
5. Initiate a checkpoint on the NHSIA Information Viewpoint artifacts.
6. Work with NHSIA HS Team on creating IEPDs for the information exchanges for the TO-BE System. Leverage the identified interfaces for the TO-BE System using NIEM.
7. If, during assessment some areas are found where NHSIA is struggling and MITA is more mature in that area consider, using the MITA framework.

4 DATA GOVERNANCE

To achieve interoperability for this and other cross-agency activities, a **governance** model for a SOA must be put in place to guide sharing at both the data and web services levels, and achieve a cross-organizational consensus and understanding at the workflow (i.e., business process) level. This project will codify and execute infrastructure/data **governance**, web service **governance**, and business process **governance** models to meet the needs of the enterprise.

Data Governance for data exchanges will directly/indirectly (unknown yet) operate under existing NIEM HS Domain Data Governance Structure so that the Data is governed at the National level.

However to govern the data that are within the premises of the agencies we will need to focus on scope, processes, policies and procedures, and roles under data governance. Under Data Governance we will also be working on the governance of data for exchanges that might not be covered by NIEM HS Governance structure.

Data Governance (see Figure 22) encompasses the people, processes and procedures required to create a consistent, enterprise view of an organization's data to:

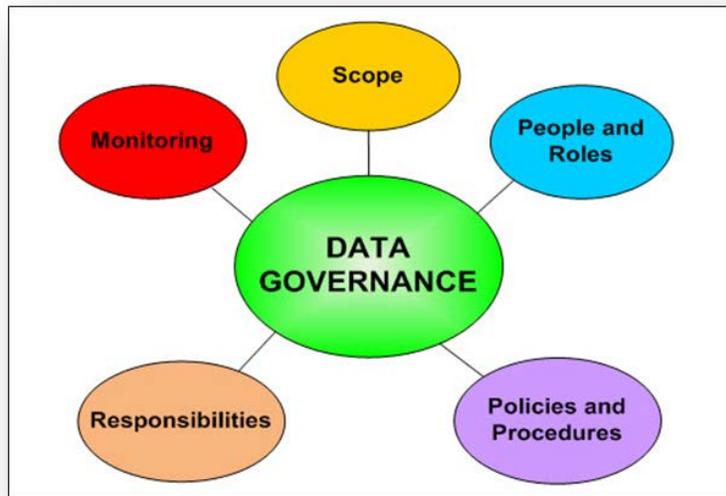


Figure 22: Data Governance

- Promote information sharing
- Improve confidence and trust in data used in decision-making
- Make information accessible, understandable, and reusable
- Reduce cost and duplication
- Improve data security and privacy

Some of the principles of Data Governance are:

- Accountability
- Transparency
- Compliance Enforcement
- Collaboration
- Data Integrity
- Stewardship
- Change Management

4.1 Mission and Vision

- Proactively define/align rules
- Provide ongoing, boundary-spanning protection and services to data stakeholders
- React to and resolve issues arising from non-compliance with rules

4.2 Goals/Metrics

Goals of data governance:

- Increase revenue and value

- Manage cost and complexity
- Ensure survival through attention to risk and vulnerabilities: compliance, security, privacy, data quality etc.

Metrics:

- If we use the Medical Eligibility and Enrollment area of Business, we should expect an interoperable system that covers the exchanges of major pieces of information between all of the participating agencies/lines of business.
- If we use the eMPI metrics, we should expect an overall reduced cost and complexity for data management, with one a one Master Person Index that is shared throughout the agency; otherwise we should expect a fragmented system, with an increase in the overall cost and complexity of implementation and maintenance.
- If we use compliance to enterprise wide standards, we should expect the data to be less vulnerable, resulting in a secure database environment resulting in a system that is less prone to attacks from the outside world and more secure data and processes. By using standardization we also increase the legibility of data because of the commonly used terminologies and processes.

Data Governance specifically helps establish strategy, objectives and policy to effectively manage enterprise data by specifying accountability on data and its related processes including decision rights. For example, Data Governance defines who owns the data; whoever creates records; who can update them; and also, who arbitrates decisions when data management disagreements arise.

Lack of data governance leads to issues such as:

- Fragmentation that leads to inefficiency and duplication of efforts and costs
- Disappointing levels of data quality
- Frequent unavailability of vital information
- High costs that grow at an unsustainable rate
- Overall lack of enterprise perspective

4.3 Challenges of Data Governance

Assessment of all participating agencies leads to believe that participating agencies currently have little or no data governance model defined. The Business Rules are not defined / documented properly. Governing bodies for the agencies are not in place. Some Policies/Rules do exist in the current environment for the data exchanges but very little are documented. At this stage, when we try to plan for/implement data governance there could be many challenges. Some of the challenges that we could face:

- Determining the rules and requirements; interpreting and understanding the rules concerning data sources
- Gaining agreement of all parties regarding policies

- Developing new tools and software to enable data governance
- The cost of implementing policies
- Incompatible systems
- Competing for priorities within the organization
- Getting management to understand what is necessary
- Building the project process

It's also good to take a look at some of the reasons that Governance cannot succeed (reasons for failure while implementing) so that we can take precautionary measures if needed. Some of the reasons in which data governance fail are:

- Cultural barriers
- Lack of senior-level sponsorship
- Underestimating the amount of work involved
- Long on structure and policies, short on action
- Lack of business commitment
- Lack of understanding that business definitions vary
- Trying to move too fast from no-data governance to enterprise-wide data governance

4.4 Organization Levels and Roles for Implementing Data Governance

Executive Level – Data Governance Board or IT Steering Committee:

- Sponsorship
- Strategic Direction
- Funding
- Advocacy
- Oversight

Judicial Level – Business and technology leaders:

- Strategic planning activities
- Enforce governance activities and policies
- Mediate disagreements about governance

Legislative Level – Chaired by a senior business leader designated by executive leadership:

- Members from business and technology leadership
- Establish data governance policy traceable to enterprise business strategies
- Establish policies for managing structured and unstructured data
- Commit resources to data governance
- Establish data stewardship programs
- Identify gaps in policies
- Escalate unresolved issues to the Judicial Level

Administrative Level – Implementers of data governance:

- Carry out data governance policies
- Clearly articulate business drivers
- Overcome inhibitors to progress
- Clarify steps to make progress at the organization, system, project and program levels
- Manage specific subject areas
- Develop data models and vocabularies
- Implement master data management best practices
- Organize content and records management
- Preservation, digital archives and long term access to data and information
- Implement data security and access policies
- Institute and monitor data quality processes
- Tracking governance related metrics
- Recommend standards and policies to the Legislative Level
- Oversee subject level data stewards who implement governance policies and standards and maintain data quality metrics

Figure 23 below shows the State’s Enterprise IT Governance Model.

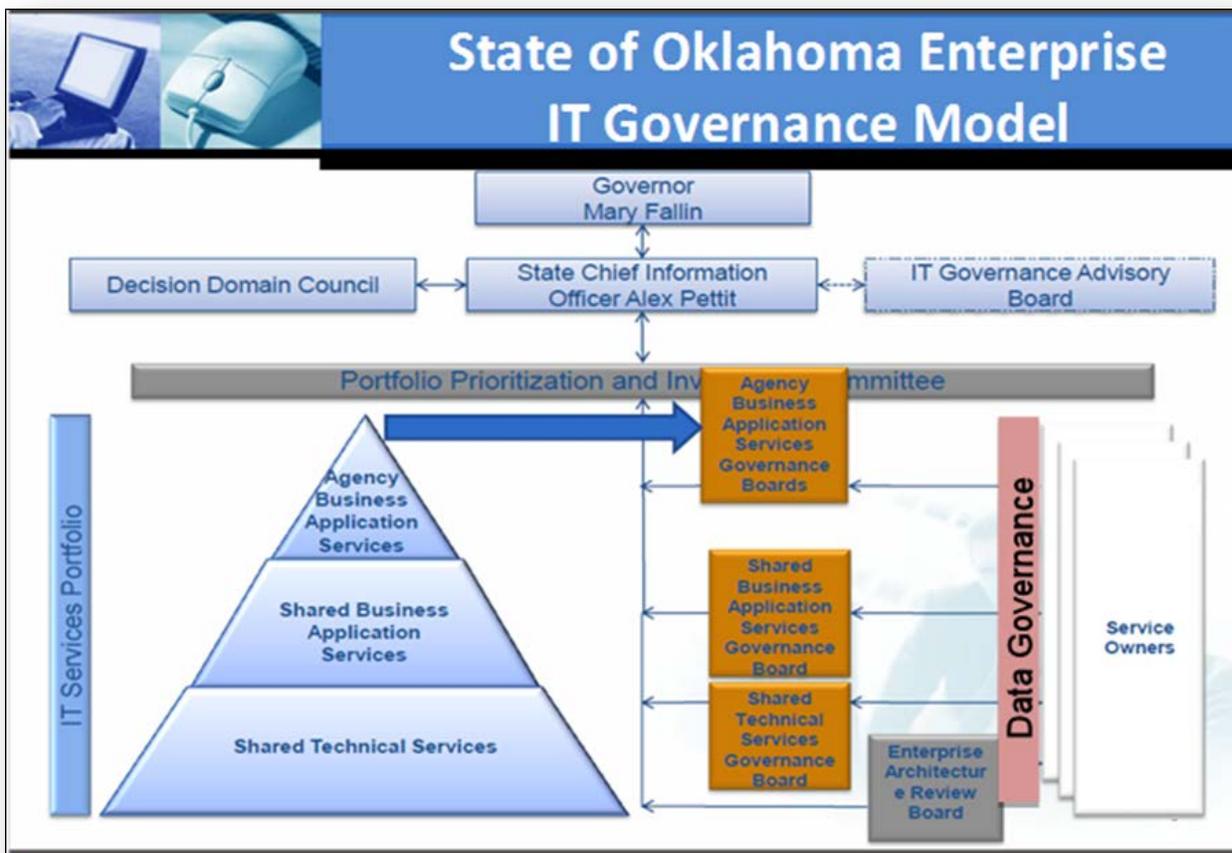


Figure 23: State of Oklahoma Enterprise IT Governance Model

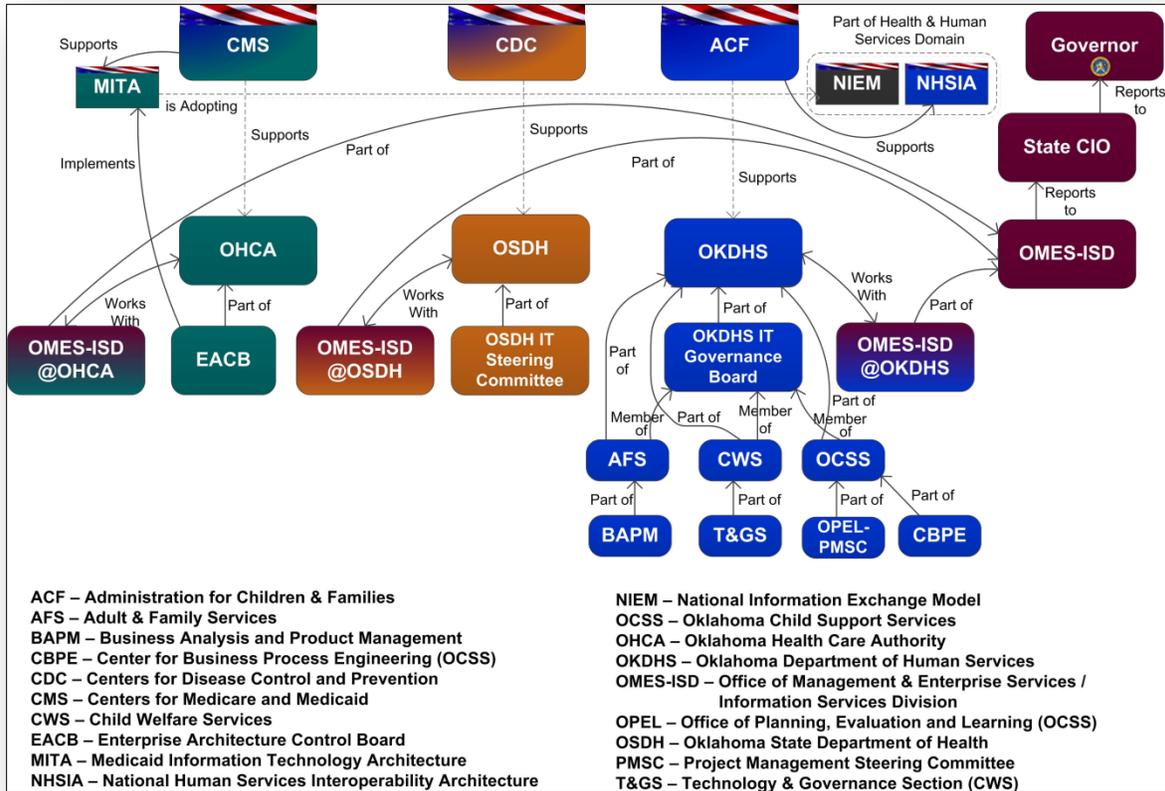


Figure 24: State of Oklahoma's Current Governance Structure

Figure 24 depicts a summary of the state's enterprise IT governance structures.

4.5 Components of Data Governance

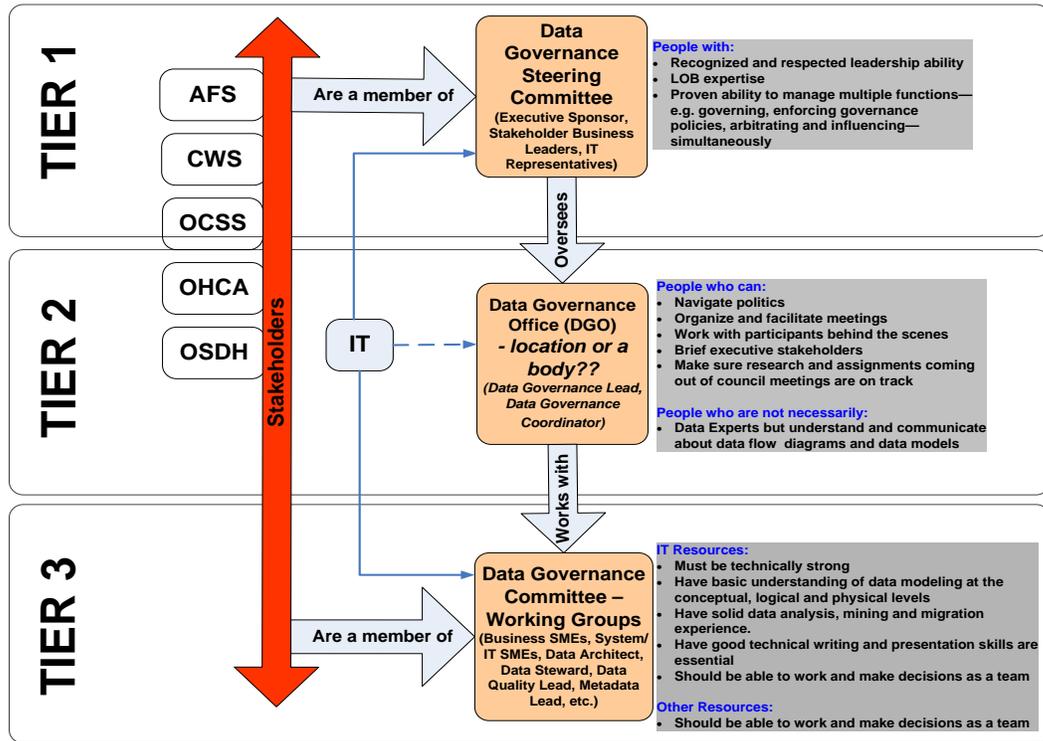


Figure 25: Recommendation for TO-BE Data Governance Structure

Components of Data Governance:

- Data Governance Committee (and Office/Location)
- Oklahoma Healthcare Authority
- Oklahoma State Department of Health
- Adult and Family Services
- Child Welfare Services
- Oklahoma Child Support Services
- Federal Agencies
- All other Stakeholders like Communities of interest
- Other State Agencies

Figure 26 below shows the Data Governance components and the data that we plan to govern. When approaching data governance plan is to focus on eMPI data first. With good Data Governance and MDM technology we can contribute to services that are less error prone, have better performance and delivery times through interoperability. These components are at a high level, e.g. OKDHS, if we go a level deep would show more stakeholders like developers, architects, program managers, database administrators etc.

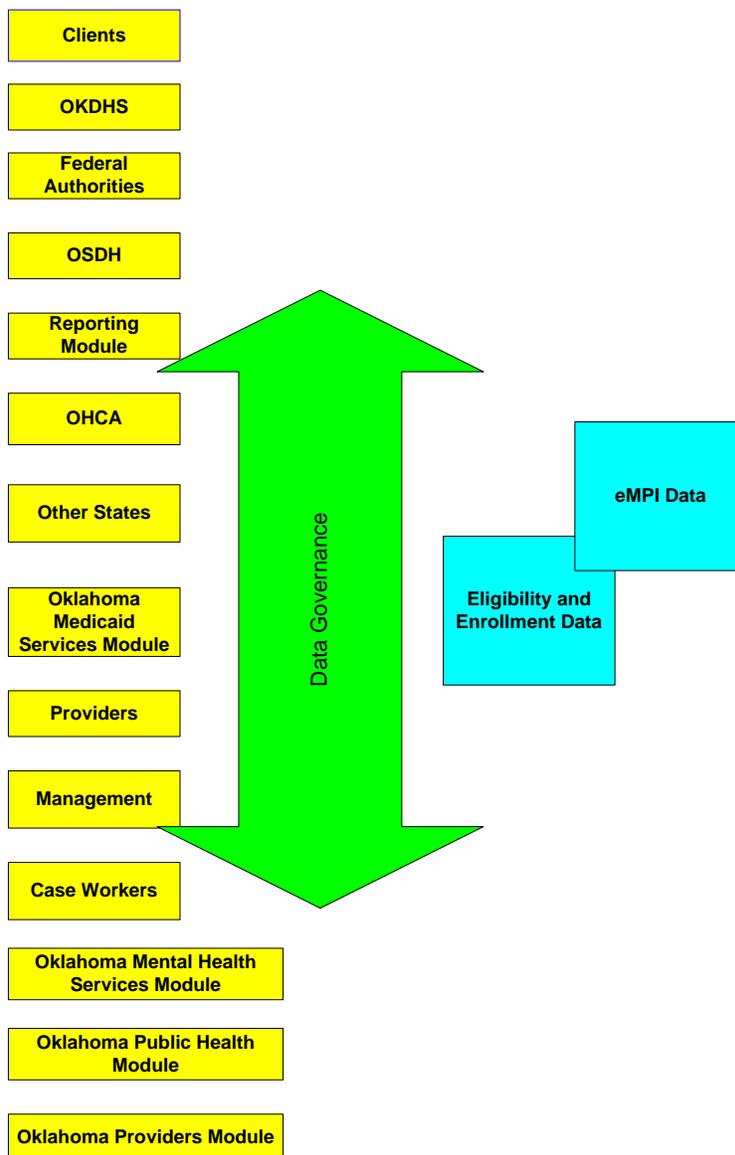


Figure 26: Data Governance Components

4.6 Data Governance Maturity Models

Various Data Governance Maturity Models is being researched and compared to assess which one would best fit our needs. Data governance comprises of maturity model and data governance framework. How to get from the maturity level that we are in to the framework that we want to support is the roadmap for data governance.

4.6.1 Gartner EIM Data Governance Maturity Model

Table 7: Gartner EIM Data Governance Maturity Model

	Level of Maturity	Characteristics
0	Unaware	<ul style="list-style-type: none"> • Strategic decision made without adequate information • Lack of formal information architecture, principles, or process for sharing information • Lack of information governance, security and accountability • Lack of understanding of meta data, common taxonomies, vocabularies and data models
Action Item: Architecture staff and strategic planners should informally educate IT and business leaders on the potential value of EIM, and the risks of not having it, especially legal and compliance issues.		
1	Aware	<ul style="list-style-type: none"> • Understanding of the value of information • Issues of data ownership • Recognized need for common standards, methods and procedures • Initial attempts at understanding risks associated with not properly managing information
Action Item: Architecture staff needs to develop and communicate EIM strategies and ensure those strategies align with [the state government] strategic intent and enterprise architecture.		
2	Reactive	<ul style="list-style-type: none"> • Business understands the value of information • Information is shared on cross–functional projects • Early steps toward cross–departmental data sharing • Information quality addressed in reactive mode • Many point to point interfaces • Beginning to collect metrics that describe current state
Action Item: Top management should promote EIM as a discipline for dealing with cross–functional issues. The value proposition for EIM must be presented through scenarios and business cases.		
3	Proactive	<ul style="list-style-type: none"> • Information is viewed as necessary for improving performance • Information sharing viewed as necessary for enabling enterprise wide initiatives. • Enterprise information architecture provides guidance to EIM program • Governance roles and structure becomes formalized • Data governance integrated with systems development methodology
Action Item: Develop a formal business case for EIM and prepare appropriate presentations to explain the business case to management and other stakeholders. Identify EIM opportunities within business units [agencies and divisions].		
4	Managed	<ul style="list-style-type: none"> • The enterprise understands information is critical • Policies and standards are developed for achieving consistency. These policies and standards are understood throughout the enterprise • Governance organization is in place to resolve issues related to cross–functional information management • Valuation of information assets and productivity metrics are developed
Action Item: [Agency and division] information management activities should be inventoried and tied to the overall [state government] EIM strategy. EIM must be managed as a program not a series of projects. Chart progress using a balanced scorecard for information management.		
5	Effective	<ul style="list-style-type: none"> • Information value is harvested throughout the information supply chain • Service level agreements are established • Top management sees competitive advantage to be gained by properly exploiting information assets • EIM strategies link to risk management, productivity targets • EIM organization is formalized using one of several approaches similar to project management. The EIM organization coordinates activities across the enterprise
Action Item: Implement technical controls and procedures to guard against complacency and to sustain information excellence even as the [state government] changes.		

Gartner developed their maturity model to provide guidance to organizations that are serious about managing information assets. It is important to understand this maturity model accompanies Gartner's definition of enterprise information management (EIM). This maturity model also presents action items for each level of maturity (Table 7) Gartner's EIM concept presents an integrated, enterprise wide approach to managing information assets and has five major goals that comprise an EIM discipline:

- Data Integration Across the Portfolio
- Unified Content
- Integrated Master Data Domains
- Seamless Information Flows
- Metadata Management and Semantic Reconciliation

4.6.2 Kalido Data Governance Maturity Model

	Organization				
	Authority	Data Stewardship	Business Role	Collaboration	
	No official authority for data; administrators for applications serve as the closest substitute.	A formal group such as Data Architecture within IT has some control over data but lacks the necessary authority to change business processes.	A council or board with high-level representation from some business functions. The council has the authority to change some business processes.	A cross-organizational council or board with institutionalized, enterprise-wide authority for all key decisions involving data.	
	No data steward role. Traditional IT is the de facto steward of data.	Informal data experts perform some of the tasks of stewardship, but their roles and responsibilities are not explicitly established.	Formal data steward roles are defined and designated for some key data areas with clearly prescribed day-to-day activities.	Data stewards are clearly designated for all key data areas. Stewards are highly visible focal points for data.	
	Business has no clear role except to provide initial requirements for application development.	Business fully participates in and sometimes leads projects, but its involvement is project-based rather than permanent.	Business is engaged in a sustained way in managing data and data policies. Some end-to-end process owners take an active role in making data policies.	Business takes full responsibility for data content and for data policy making.	
	Rigid boundary exists between business and IT with little collaboration.	Collaboration clearly exists. It is intense during a major initiative but is ad hoc on a day-to-day basis.	Business-IT collaboration on data is institutionalized as a routine activity even in the absence of a major initiative.	Business-IT collaboration related to data is pervasive throughout the enterprise.	
	Traditional IT is completely accountable for data, but accountability is not aligned with business objectives.	Traditional IT is accountable for data, and accountability is somewhat aligned with business objectives.	Accountability for data and its quality is documented and assigned to the most appropriate individuals, typically not IT. However, there is typically no way to enforce accountability.	Accountability for data is institutionalized with common, measurable performance metrics tied to employee performance.	
	Data is a by-product of business activities and not valued until someone needs it.	Intuitive awareness that data is an asset, but the organization lacks a framework to determine the relative value of different types of data.	The concept of data as an asset has emerged; data is valued, and activities are prioritized based on business impact.	Pervasive culture of treating data as a strategic enterprise asset with quantifiable value.	
Process	Policy Management	No concept of data policies. Rules for data are embedded in application logic and are not accessible.	Loose and informal processes for data governance centered around major systems. The processes tend to degrade over time and are impossible to audit.	Transparent processes for managing cross-system data policies are established. End-to-end process satisfies auditors and regulators.	Data governance, including policy definition, implementation and enforcement is a core business process in its own right.
	Communication	Communication occurs during system deployment and training.	Communication is infrequent and often in response to a crisis. It takes time and determination to discover policies.	New and updated data policies are communicated to the people impacted; they are easily accessible when needed.	Data policies pop up in context when applicable, and users are guided on how data should be created, used and handled.
	Issue Resolution	There is no way to raise data issues.	An official channel for raising data issues exists but is not effective. Most problems are resolved through informal networks.	Issues are recorded, reported and tracked through to resolution by data stewards working in collaboration with business and IT.	Potential issues are identified in real time and remediated collaboratively before they can negatively impact the business.
	Decision Rights	Decisions for data are primarily made by IT.	Decision-making is system specific and unstructured at the enterprise level.	Decision-making is structured and decision rights are clearly defined and communicated.	Decision-making for data is institutionalized and made with full understanding of the quantifiable benefit-cost-risk trade-offs.
	Performance Management	No performance management.	Metrics are system specific and heavily IT operations oriented.	Some operational metrics for data governance program have been established and are tracked. They are tied to business needs.	Key metrics on efficiency and effectiveness are standardized. Actuals and goals are compared for variance.
	Dataflow Transparency	Data authors do not know who will use the data or how the data will be used. Data consumers do not know where the data comes from.	IT has some documentation on dataflows from authors to consumers, but business in general does not.	Dataflows for some core processes are documented and accessible by data authors and consumers so that they're aware of the dependencies.	Full transparency of how key enterprise data assets are produced and consumed. Data's downstream impact is well understood.
Technology	Data Policies and Rules	No concept of data policies. Rules for data are embedded in application logic and not accessible.	Policies and rules exist in loosely documented form. They are not managed through a central and easily accessible repository.	Common enterprise repository of data quality policies and rules established, accessible by all stakeholders including business and IT.	Common and pervasive policy layer for data quality, security and lifecycle fully integrated with key systems.
	Process Orchestration	No data governance process exists to be supported.	Informal workflow using office desktop application and general purpose collaboration tools such as SharePoint.	Data governance processes are orchestrated by workflow with automation to guide the day-to-day activities of the extended data organization.	Data governance processes are orchestrated by workflow and integrated with enterprise workflow engine.
	Compliance Monitoring	Data consumers discover data issues during the course of use but don't know who to inform for correction.	IT uses tool-specific features (for example ETL rejection) to detect violations to rules. Data consumers don't have a way to report additional data issues.	Active monitoring is deployed and run regularly on multiple data repositories to assess compliance. Data consumers can easily raise issues.	Data quality and security monitoring against policies in place for all key data elements and run on both stored and in-flight data. Data consumers have in-system ways of alerting data stewards of errors.
	Modeling	Models exist for each application only.	IT produces bottom-up, inventory-style metadata management that lacks business visibility and control. Top-down models are not actively used.	Unified and business-accessible models for data, business processes and systems strongly influence system development.	Top-down model actively drives the design and behavior of key systems.
	Master Data Management	Master data resides in disparate applications and is unmanaged.	Single or multi-domain MDM (typically for customer or product master data) is implemented but lacks governance.	Multiple MDM platforms work in concert with a central data governance application to implement and execute enterprise data policies for master data.	Master data complies with enterprise data policies and rules at the points of origin.
	Data Quality	Data quality is poor and is not measured.	IT runs data profiling and cleansing in an ad hoc manner and on narrow uses cases at the repository level.	Data quality for key data assets is measured holistically, reported and tracked over time to sustainably improve it.	Data quality metrics are pervasive and presented in context to help consumers use data effectively.
		Application-Centric	Enterprise Repository-Centric	Policy-Centric	Fully Governed



Figure 27: Kalido Data Governance Model

Like any important business capability, data governance requires organization, processes, and technology to be successful. Kalido's data governance maturity model is based on market research with more than 40 companies at varying stages of maturity. Kalido's maturity stages: Application-Centric, Enterprise Repository-Centric, Policy-Centric, and Fully Governed, map to the evolution of how organizations treat data assets. At the same time, the Kalido Data Governance Maturity Model provides milestones for organization, process and technology - which need to be aligned - to advance to a more mature stage.

Kalido provides an online assessment tool to determine where an organization stands as far as data governance goes.

4.6.3 IBM Data Governance Council Maturity Model

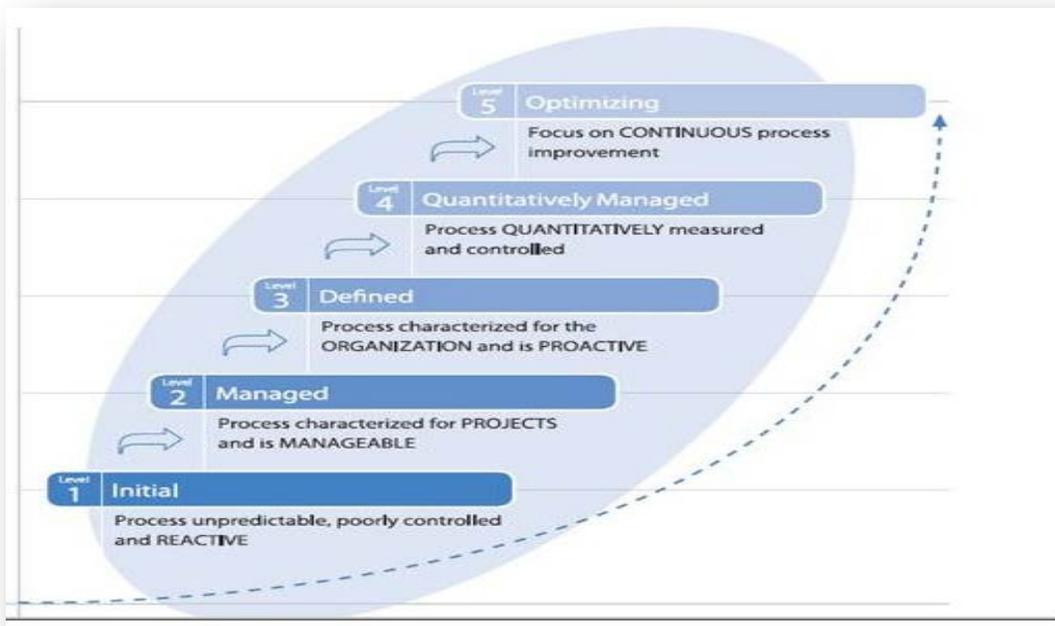


Figure 28: IBM Data Governance Council Maturity Model

IBM's data governance maturity model is based on the Software Engineering Institute (SEI) Capability Maturity Model (CMM). The Data Governance Council's Maturity Model defines a set of domains that comprise data governance.

4.7 Data Governance Frameworks

4.7.1 Data Governance Institute Framework

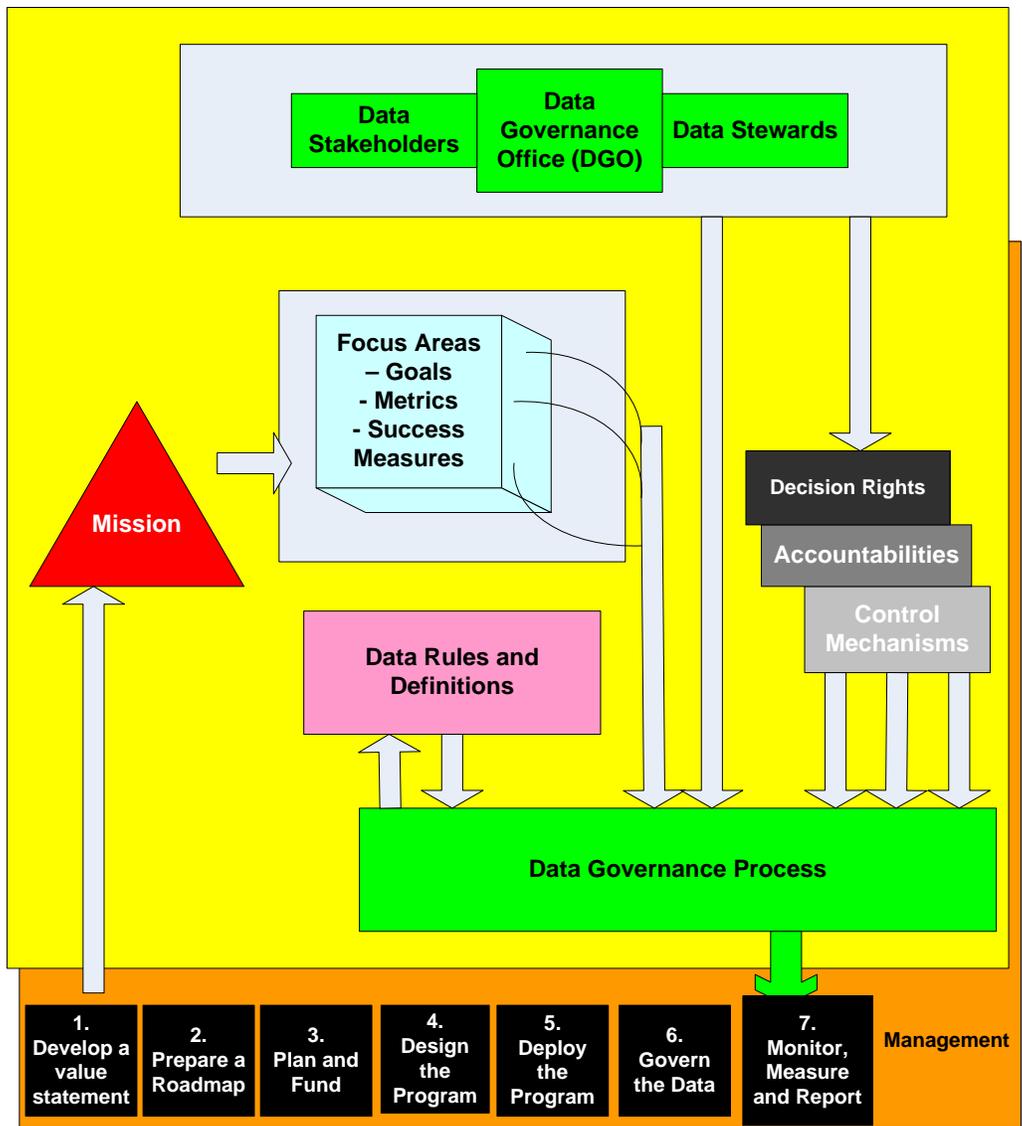


Figure 29: Data Governance Institute (DGI) Framework

Figure 29 shows the DGI Data Governance Framework that is designed to assist organizations that needs a data governance system. The framework is designed to work for corporations, government agencies, schools, and other types of organizations that work with data.

In complex scenarios where many organizations are involved, it's not easy to identify - much less meet - all data stakeholders' information needs:

- Some of those stakeholders are concerned with operational systems and data
- Some are concerned about analysis, reporting, and decision-making
- Some care primarily about data quality, while others are frustrated by architectural inadequacies that keep users from linking, sorting, or filtering information
- Some data stakeholders focus on controlling access to information; others want to increase abilities to acquire and share data, content, documents, records, and

reports. And still others focus on compliance, risk management, security, and legal issues

Each of these data stakeholder groups may have a different vocabulary to describe their needs, their drivers, and their constraints. Indeed, they may not even have the same set of requirements in mind when they call for better governance of data.

Frameworks help us organize how we think and communicate about complicated or ambiguous concepts.

The Data Governance Institute wanted to introduce a practical and actionable framework that could help a variety of data stakeholders from across any organization to come together with clarity of thought and purpose as they defined their organization's Data Governance and Stewardship program and its outputs.

4.7.2 Data Management Association (DAMA) Framework

The DAMA framework presents how data governance drives other functions that comprise an enterprise data management initiative. The DAMA framework is a set of two frameworks that encompass data management: a functional framework and an environmental element framework. The center cell in the functional framework describes governance.



Figure 30: DAMA Functional Framework

The environmental elements, which comprise the DAMA Environmental framework, are presented in Figure 31. The two component frameworks are meant to work together.



Figure 31: DAMA Environmental Framework

4.7.3 IBM Data Governance Council Framework

IBM Data Governance Council Framework (Figure 32) framework presents major concepts that comprise not only governance but also an enterprise data management practice. Major dependencies are presented across groupings of functions. The functions presented compare well with the DAMA functional framework for data management.

The IBM Data Governance Council Framework was designed to be *outcome oriented*. *Risk Management, compliance, and value creation* are seen as desirable outcomes of a data governance program, even though they may also be daily operational activities and present policy challenges. The focus in this framework is on organizational behavior based on an underlying premise that only people can be governed and *not the data itself per se*.

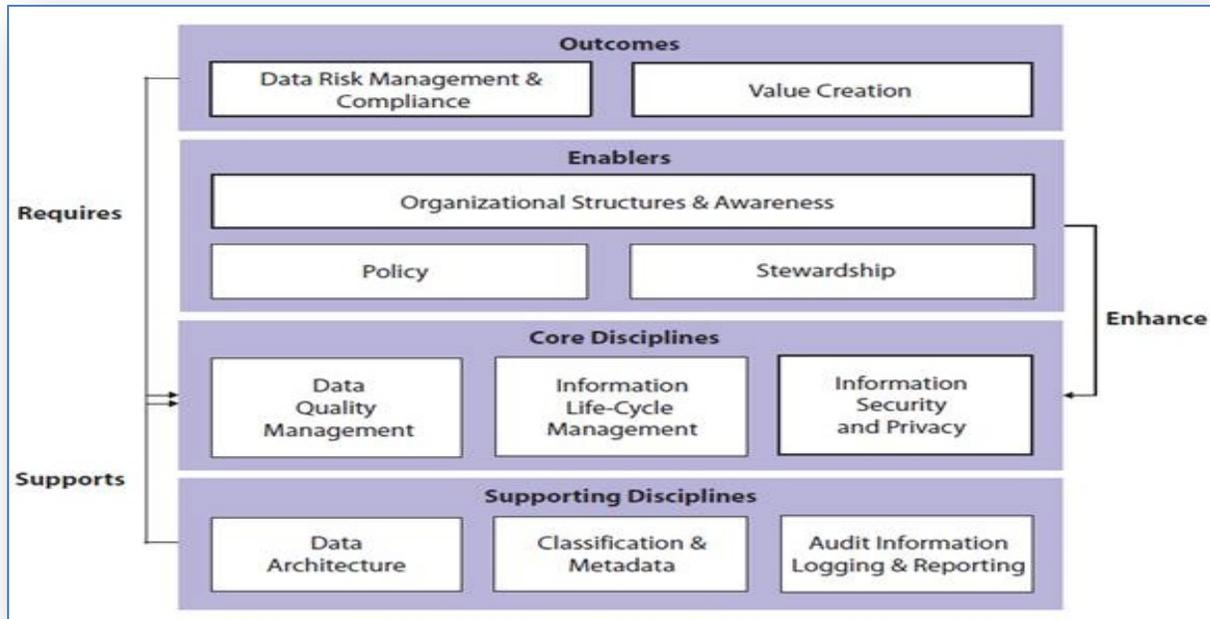


Figure 32: IBM Data Governance Framework - Elements of Effective Data Governance

4.8 Data Stewardship

Data stewardship is the management and oversight of corporate data by designated personnel who typically don't own the data but are responsible for tasks such as developing common data definitions and identifying data quality issues. The Data Stewardship (or Governance) Council consists of a set of Data Stakeholders who come together to make data related decisions. They may set policy and specify standards, or they may craft recommendations that are acted on by a higher-level governance board. Specific responsibilities of Data Stewards would include:

- Access Procedure
- Create Policies and Verify Compliance to Policies
- Coordination
- Documentation
- Communication
- Data Quality, integration and correction
- Data lifecycle and retention
- Data Storage
- Education to Employees on data quality
- Data Classification based on some criteria e.g. risk, sensitivity.

4.9 Assessment of Maturity Levels of Agencies

Based on the data from the agencies, Kalido's assessment table was used to assess the general level that the agencies are in. The assessment is in Table 8. The level that we seem to be in is highlighted. All agencies fall under level 1 or 2. Kalido's model was used for assessment purposes because it has detail coverage of the areas of data governance.

90FQ0006 Oklahoma Interoperability Grant Project
Data Road Map, Revision 2.0, April 26, 2013

Table 8: Assessment result on data governance maturity level

	1	2	3	4
Authority	Not really defined; taking the initiator of the data as the 'owner' having authority	A formal group such as Data Architecture within IT has some control over data but lacks the necessary authority to change business processes	A council or board with high-level representation from some business functions. The council has the authority to change some business processes.	A cross-organizational council or board with institutionalized, enterprise-wide authority for all key decisions involving data.
Data Stewardship	No Data Steward Role. IT personnel from agencies form the de facto Data Stewards.	Informal data experts perform some of the tasks of stewardship, but their roles and responsibilities are not explicitly established	Formal data steward roles are defined and designated for some key data areas with clearly prescribed day-to-day activities.	Data stewards are clearly designated for all key data areas. Stewards are highly visible focal points for data.
Business Role	Business is involved in most of the projects; but business requirements are not clearly defined in the beginning and are updated as the project moves forward.	Business fully participates in and sometimes leads projects, but its involvement is project-based rather than permanent.	Business is engaged in a sustained way in managing data and data policies. Some end-to-end process owners take an active role in making data policies.	Business takes full responsibility for data content and for data policy making.
Collaboration	Business/ IT activities within a project have some collaboration but many other processes that the project are dependent on are running on siloes	Collaboration clearly exists. It is intense during a major initiative but is ad hoc on a day-to-day basis.	Business-IT collaboration on data is institutionalized as a routine activity even in the absence of a major initiative.	Business-IT collaboration related to data is pervasive throughout the enterprise.
Accountability	IT is accountable for data but accountability is not aligned with business objectives	Traditional IT is accountable for data, and accountability is somewhat aligned with business objectives	Accountability for data and its quality is documented and assigned to the most appropriate individuals, typically not IT. However, there is typically no way to enforce accountability.	Accountability for data is institutionalized with common, measurable performance metrics tied to employee performance.
Cultural Attitude	Data is not given much value until someone needs it.	Intuitive awareness that data is an asset, but the organization lacks a framework to determine the relative value of different types of data	The concept of data as an asset has emerged; data is valued, and activities are prioritized based on business impact.	Pervasive culture of treating data as a strategic enterprise asset with quantifiable value.
Policy Management	Not much on data policies. Database standards exist and Data Naming conventions standard exist but they exist for the agency, they are not enterprise wide standards. Some of the rules are embedded in the application	Loose and informal processes for data governance centered around major systems. The processes tend to degrade over time and are impossible to audit.	Transparent processes for managing cross-system data policies are established. End-to-end process satisfies auditors and regulators.	Data governance, including policy definition, implementation and enforcement is a core business process in its own right.
Communication	Communication occurs during system deployment and training	Communication is infrequent and often in response to a crisis. It takes time and determination to discover policies. Communication is project-centric. It's not there at the enterprise-wide level except for some trainings and information sharing sessions	New and updated data policies are communicated to the people impacted; they are easily accessible when needed.	Data policies pop up in context when applicable, and users are guided on how data should be created, used and handled.
Issue Resolution	There is no way to raise data issues	An official channel for raising issues exists but some lines of business use their own process for raising/resolving issues. Helpdesk is the centralized issue raising system.	Issues are recorded, reported and tracked through to resolution by data stewards working in collaboration with business and IT.	Potential issues are identified in real time and remediated collaboratively before they can negatively impact the business.
Decision Rights	Decisions for data are primarily made by IT	Decision-making is system-specific and unstructured at the enterprise level.	Decision-making is structured and decision rights are clearly defined and communicated.	Decision-making for data is institutionalized and made with full understanding of the quantifiable benefit-cost/risk trade-offs.
Performance Management	No performance management	Metrics are system specific and heavily IT operations oriented. There is a specific group that monitors performance and also checks performance upon request	Some operational metrics for data governance program have been established and are tracked. They are tied to business needs.	Key metrics on efficiency and effectiveness are standardized. Actuals and goals are compared for variance.
Dataflow Transparency	Data Authors not know who will use the data or how the data will be used. Very little documentation. Data consumers do not know where the data comes from	IT has some documentation on dataflows from authors to consumers. Data Authors not always know how the data will be used	Dataflows for some core processes are documented and accessible by data authors and consumers so that they're aware of the dependencies.	Full transparency of how key enterprise data assets are produced and consumed. Data's downstream impact is well understood.
Data Policies and Rules	No concept of data policies.	Policies and rules exist in loosely documented form. They are not managed through a central and easily accessible repository. Database and Data naming standards exist for the agency, but they are not enterprise-wide standards. Some of the rules are embedded in the application	Common enterprise repository of data quality policies and rules established, accessible by all stakeholders including business and IT.	Common and pervasive policy layer for data quality, security and lifecycle fully integrated with key systems.
Process Orchestration	No Data Governance Process is in place to be supported	Informal workflow using office desktop application and general purpose collaboration tools such as Sharepoint	Data governance processes are orchestrated by workflow with automation to guide the day-to-day activities of the extended data organization.	Data governance processes are orchestrated by workflow and integrated with enterprise workflow engine.
Compliance Monitoring	Data consumers discover data issues during the course of use but don't know who to inform for correction	IT uses tool-specific features to detect violations to rules. Data consumers have the Helpdesk/or their own issue raising template to raise data issues	Active monitoring is deployed and run regularly on multiple data repositories to assess compliance. Data consumers can easily raise issues.	Data quality and security monitoring against policies in place for all key data elements and run on both stored and in-flight data. Data consumers have in-system ways of alerting data stewards of errors.
Modeling	Data Models exist for most of the applications	IT produces bottoms-up, inventory-style metadata management that lacks business visibility and control. Top-down models are not actively used.	Unified and business-accessible models for data, business processes and systems strongly influence system development.	Top-down model actively drives the design and behavior of key systems.
Master Data Management	Master Data Management Procedure is not in place yet. They are segregated and duplicated throughout the applications	Single or multi-domain MDM is implemented but lacks governance	Multiple MDM platforms work in concert with a central data governance application to implement and execute enterprise data policies for master data.	Master data complies with enterprise data policies and rules at the points of origin.
Data Quality	Data Quality is not measured; might be measured in cases where certain application is going through the performance checking process by the Performance team	IT runs data profiling and cleansing in an ad hoc manner on narrow use cases at the repository level	Data quality for key data assets is measured holistically, reported and tracked over time to sustainably improve it.	Data quality metrics are measured and presented in context to help consumers use data effectively.
	Application Centric	Enterprise Repository Centric	Policy Centric	Fully Governed

4.10 Policies and Procedures (Data Security, Data Access, Data Reusability, Data Integrity, Data Deduplication)

Policies and Procedures related to data exchanges:

1. **Federal (from IRS Pub 1075):** Used for all FTI transactions to OKDHS.
 - FTI (Federal tax Returns and Returns Information) is disclosed only to authorized persons and used only as authorized by the statute or regulation.
 - Requirements apply to all organizational segments of an agency receiving FTI.
 - The receiving agency must show, to the satisfaction of the IRS, the ability to protect the confidentiality of the information.
 - An agency must ensure its safeguards will be ready for immediate implementation upon receipt of FTI.
 - Copies of the initial and subsequent requests for data and of any formal agreement must be retained by the agency a minimum of five years as a part of its record keeping system.
 - Safeguards must be designed to prevent unauthorized access and use.
 - Besides written requests, the IRS may require formal agreements that specify, among other things, how the information will be protected.
 - Agencies should always maintain the latest Safeguard Procedures Report (SPR) on file.
 - SPR must be submitted to the IRS at least 45 days before the scheduled or requested receipt of FTI.
 - Multiple organizations, divisions or programs within one agency using FTI. may be consolidated into a single report for that agency, with permission of the Office of Safeguards.
 - Any agency that receives FTI for an authorized use may not use that information in any manner or for any purpose not consistent with that authorized use.
 - The IRS has established a Secure Data Transfer (SDT) program to provide encrypted electronic transmission of FTI between the IRS and trading partners.

2. **Safeguard Activity Rules (SAR):** Used for FTI exchanges with Feds and OKDHS Divisions AFS and OCSS:
 - Agencies shall submit their SAR on the template developed by the IRS Office of Safeguards.
 - IRS Office of Safeguards does not accept hard copy submissions.
 - The SAR should be accompanied by a letter on the agency's letterhead signed and dated by the head of the agency or delegate.
 - Always provide the agency Director or Commissioner; Information Technology Security Officer or equivalent; and the Primary IRS contact (Disclosure Officer) information. Include the name, title, mailing address, phone number and e-mail address for each individual.

- Always provide an organizational chart or narrative description of the receiving agency, which includes all functions within the agency where FTI will be received, processed, stored and/or maintained. The description should account for off-site storage, consolidated data centers, disaster recovery organizations, and contractor functions.
- Describe changes or enhancements to information or procedures previously reported impacting hardware, software, IT organizational operations (movement to state run data center), or system security.
- Describe changes or enhancements to information or procedures previously reported impacting physical layout (new location or enhancements to current location) and changes to two-barrier protection standard.
- Describe changes or enhancements to currently approved retention and disposal policy or methods (e.g. outsourced disposal to shredding company, change in shredding equipment, off-site storage procedures and changes in retention period).
- Disclosure awareness should be exposed to all employees having access to FTI (includes off-site storage, consolidated data centers, disaster recovery organizations, and contractor functions).
- Copies of a representative sampling of the Inspection Reports and a narrative of the corrective actions taken (or planned) to correct any deficiencies, should be included with the annual SAR.
- Describe the amount and method of destruction of FTI (paper and/or electronic, including backup tapes) disposed during the processing period.
- Agencies authorized to re-disclose FTI to other agencies must provide the name(s) of the agency to which they provided FTI and the number of records provided.
- The agency must attach a Corrective Action Plan (CAP) to report all corrective actions taken or planned to address findings arising from the last on-site safeguard review until all findings are closed.
- Any planned agency action that would create a major change to current procedures or safeguard considerations should be reported.
- The agency must identify all contractors with access to FTI and the purpose for which access was granted. Details of the contractors as mentioned in Section 7.4.5 in the SAR need to be supplied.
- The agency must summarize the FTI received both paper and electronic, during the reporting period, including source, name of file or extract, and volume. Record keeping log is required in Publication 1075 Section 3.
- State tax agencies using FTI to conduct statistical analysis, tax modeling or revenue projections must provide updated information regarding their modeling activities which include FTI.

3. OCSS Policies and Procedures:

- The State must have policies and procedures to evaluate the system for risk on a periodic basis.

- The system must be protected against unauthorized access to computer resources and data in order to reduce erroneous or fraudulent activities and protect the privacy rights of individuals against unauthorized disclosure of confidential information.
- The State must have procedures in place for the retrieval, maintenance, and control of the application software.
- The State must have procedures in place for the retrieval, maintenance, and control of program data.
- The system hardware, software, documentation, and communications must be protected and backups must be available.
- The system must be capable of processing date/time data.

4. **AFS Policies and Procedures:**

- Raw tax data which includes any written, typed, photocopied, or printout of information from the Income Eligibility Verification System-Internal Revenue Service (IEVS-IRS), Beneficiary and Earnings Data Exchange System (BENDEX), and Beneficiary Earnings Exchange Record (BEER):
 - (I) Must be secured in a storage area, such as a locked desk or file cabinet;
 - (II) May not be viewed or stored on any electronic device that is not the property of OKDHS or the State of Oklahoma; OKDHS – OAC 340:65-1-2. Confidential nature of case material, Page 1 of 6.
<http://www.okdhs.org/library/policy/oac340/065/01/0002000.htm>
3/5/2013
 - (III) May not be printed or maintained in a non-electronic format;
 - (IV) May not be sent via e-mail; and
 - (V) May not be transmitted via fax; and reasonable privacy or restricted viewing of electronic data visible on computer screens or mobile devices.
- Raw tax data is viewed on the PS2 eligibility system through the IEV and BWG transactions, this information should not be printed unless authorized by legal staff.
- OKDHS enters into different types of information sharing agreements or contracts with outside agencies. The AFS Information Privacy and Security Section maintain such agreements or contracts. HSC staff sends inquiries regarding release of such information to the AFS Information Privacy and Security Section or emails FSSDSecurity@okdhs.org to determine what, if any, information may be released.

5. **OHCA Business Rules for Data Exchanges: General Policies and Procedures:**

- OHCA and the participants enter into mutual agreement by signing the documents and agree to the policies and procedures as defined in the Data Use Agreement Form and Business Associate Agreement Form.

- Any change to the Data Exchange process goes through a Change Order process.
6. **OKDHS maintains the following security measures on data (as Defined in Policy OKDHS: 2-41-15 Data Security):**
- **General policy:** All data collected and maintained by Oklahoma Department of Human Services (OKDHS) is owned by and becomes the responsibility of OKDHS.
 - **Delegation of data ownership:** For the purposes of interpreting confidentiality restrictions imposed by law, establishing data classification, and approving access to data, ownership of data is delegated by OKDHS to the OKDHS division director, whose division collects and maintains the data.
 - **Classification:** All data is classified as either confidential or non-confidential data.
 - **Assignment of responsibilities:** Data security administration consists of three primary entities which are in turn supported by several functional area entities. The three primary entities are the data owner, the decentralized security representative (DSR), and ETS Security Services.
 - **Functional responsibilities:** Functional Responsibilities are defined for each Section.
 - **Remote Access.**
 - **Virus protection:** All workstations and servers connected to the OKDHS network have Terminate and Stay Resident (TSR) anti-virus software installed on them.
 - **LAN security:** DSD Security Services Section assists divisions with security issues and requirements for LANs.
 - **Network security:** All networks that have accessibility to OKDHS data are subject to compliance with OKDHS data security guidelines documented in these regulations.
 - **Outgoing Internet usage:** Restrictions apply to the use of the Internet.
 - **Incoming Internet usage:** Processes and controls pertaining to incoming Internet usage requests are established by ETS Security Services on a case by case basis depending on the specific business need and security requirements.
 - **Mobile devices:** Users in possession of an OKDHS mobile device must comply with OKDHS Policies on Mobile Devices.
 - **E-mail usage:** The purpose of this subsection is to identify the circumstances under which a user may use the OKDHS electronic mail (e-mail) system, define what OKDHS considers acceptable use and conduct in utilizing e-mail, provide clear communication of OKDHS expectations with respect to what is and what is not acceptable use, and minimize the risk of offensive or inappropriate e-mail.

Refer to Appendix A-3 for Business Rules specific to interfaces.

4.11 Recommended Approach for Data Governance

- A Data Governance Steering Committee needs to be formed. It should fit into the State's IT Governance Model. It should include business representatives from all participating agencies. Option might be to scope this functionality within the IT steering committee that we currently have.
- A DGO needs to be established. It could be a body or a physical location. Physical location would be something similar to the PMO.
- A Data Governance Committee needs to be formed. It should include the owners of data and should focus on implementation of data governance. This is the group that would actually do the work of creating Policies and Procedures. These include the data stewards.
- A Data Governance Maturity Model should be established. An existing Data Governance Maturity model can be used if it reflects our AS-IS stage in data governance. Results of a preliminary assessment of the AS-IS situation is shown in Table 10.

5 REFERENCED DOCUMENTS

In the event of conflict between these reference documents and contents of this document, contents of this document shall be considered a superseding requirement.

5.1 Government Documents

NASCIO: Representing Chief Information Officers of the States. Data Governance – Managing Information As An Enterprise Asset Part I – An Introduction. NASCIO Governance Series.

NASCIO: Representing Chief Information Officers of the States. Data Governance Part II – Maturity Models – A Path to Progress. NASCIO Governance Series.

NASCIO: Representing Chief Information Officers of the States. Data Governance Part III – Frameworks – Structure for Organizing Complexity. NASCIO Governance Series.

Gwen Thomas. The Data Governance Framework. The Date Governance Institute.

DataGovernance.com[online]. Date Governance Institute.
http://www.datagovernance.com/fw_the_DGI_data_governance_framework.html

Winston Chen. Kalido Data Governance Maturity Model. Kalido White Paper.

Janne J. Korhonen. MDM and Data Governance. SoberIT Software Business and Engineering Institute, Helsinki University of Technology.

John Radcliffe. The Seven Building Blocks of MDM: A Framework for Success. Gartner Publications.

90FQ0006 Oklahoma Interoperability Grant Project
Data Road Map, Revision 2.0, April 26, 2013

Guidance for Exchange and Medicaid Information Technology (IT) Systems. Centers for Medicare and Medicaid Services.

Bill Branch. HL7 MITA Project and the MITA Information Architecture, Centers for Medicare and Medicaid Services. 2008 MMIS Conference, September 14-18, Nashville, TN.

MITA Information Series. Centers for Medicare and Medicaid Services.

Eric Sweden. A National Framework for Collaborative Information Exchange: What is NIEM? NASCIO – National Information Exchange Model Initiative. NASCIO representing Chief Officers of the States.

MITA Modeling Training Package. Medicaid.Gov.

Integration and Interoperability Across Public Health, Human Services, and Clinical Systems. NACCHO, May 3rd, 2012.

National Human Services Interoperability Architecture. Information Viewpoint Description, Draft Version D0.2, Prepared for Administration for Children and Families (ACF), June 2012.

David Jenkins. ACF Interoperability Human Services 2.0 Overview, August 2011.

National Human Services Interoperability Architecture (NHSIA) Definition [online]. Administration for Children and Families.
<http://www.acf.hhs.gov/nhsia-definition>

NHSIA Webinar Series, 2012.

NHSIA How the Client and Case Management are Addressed in NHSIA White Paper

National Human Services Interoperability Architecture. Eligibility White Paper, Draft Version D0.2, Prepared for Administration for Children and Families (ACF), June 2012.

NHSIA Systems Viewpoint artifact, Services Invoked by Applications

NHSIA Information Viewpoint

NHSIA Capability Viewpoint artifact, Performance Reference Model, Appendix B-Major Information Systems and Data Bases

NHSIA Systems Viewpoint artifact, Service Matrix

5.2 Non-Government Documents

Oklahoma Collaborative Project–Project Narrative.

Web Application iCE(Production).

<http://128.212.227.160/MMIS/Default.aspx?XDomPT=117c4851-ba59-4b62-86a1-ef76d38352f7>

Agency User Manual (No Wrong Door). See Appendix A-1-5.

6 ACRONYMS

<i>Acronym</i>	<i>Definition</i>
AFCARS	Adoption and Foster Care Analysis and Reporting System
AFS	Adult and Family Services
AOP	Acknowledgment of Paternity
APD	Advance Planning Document
BPO	Business Process Outsourcing
CFSR	Children and Family Service Reviews
CSENet	Child Support Enforcement Network
CWS	Child Welfare System
DB	Database
DDSD	Departmental Disabilities Services Division
EDI	Electronic Data Interchange
eMPI	Enterprise Master Person Index
ESB	Enterprise Service Bus
FACS	Family Assistance/Client Service
FIDM	Federal Institution Data Match
FTP	File Transfer Protocol
HNC	Healthcare Network Cloud
HPES	Hewlett Packard Enterprise Service
HAS	Health Services Application
IT	Information Technology
IVR	Integrated Voice Response
JOLTS	Office of Juvenile Affairs for Juvenile Criminal Histories
LIHEAP	Low-Income Home Energy Assistance Program
LPAR	Logical Partition
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
NASIRE	National Association of State Information Resource Executives
NCANDS	National Child Abuse and Neglect Data System
NIEM	National Information Exchange Model
NHSIA	National Human Services Interoperability Architecture
NYTD	National Youth in Transition Database
OCS	Oklahoma Children's Services
OCSE	Office of Child Support Enforcement
OCSS	Oklahoma Child Support Services

90FQ0006 Oklahoma Interoperability Grant Project
 Data Road Map, Revision 2.0, April 26, 2013

Acronym	Definition
OEMS-ISD	Oklahoma Office of Management and Enterprise Services – Information Services Division
OESC	Oklahoma Employment Security Commission
OHCA	Oklahoma Healthcare Authority
OKDHS	Oklahoma Department of Human Services
OSDH	Oklahoma State Department of Health
OSF	Oklahoma Office of State Finance
OSIS	Oklahoma Support Information System
PARB	Post Adjudication Review Board
PHOCIS	Public Health Oklahoma Client Information System
RFP	Request for Proposal
RFQ	Request for Quote
SAN	Storage area network
SDLC	Software Development Life Cycle
SFTP	Secure File Transfer Protocol
SMI	Structure of Management Information
SNAP	Supplemental Nutrition Assistance Program
SOA	Service Oriented Architecture
SSA	Social Security Administration
SSI	Supplemental Security Income
SSN	Social Security Number
TANF	Temporary Assistance for Needy Families
UI	User Interface
UIB Data	Utility Integration Bus
VPN	Virtual Private Network
WIC	Women, Infant and Children

- AS-IS SYSTEM OVERVIEW

Figure A-1 shows the interactions between Oklahoma Department of Human Services (OKDHS) agencies (e.g., PS2 - Adult and Family Services (AFS), Oklahoma Support Information System (OSIS) - Oklahoma Child Support Services (OCSS), KIDS – Child Welfare Support (CWS)), and other departments and organizations (e.g., OHCA - Medicaid Management Information System (MMIS), Office of Management and Enterprise Services (OMES), Oklahoma State Department of Health (OSDH)).

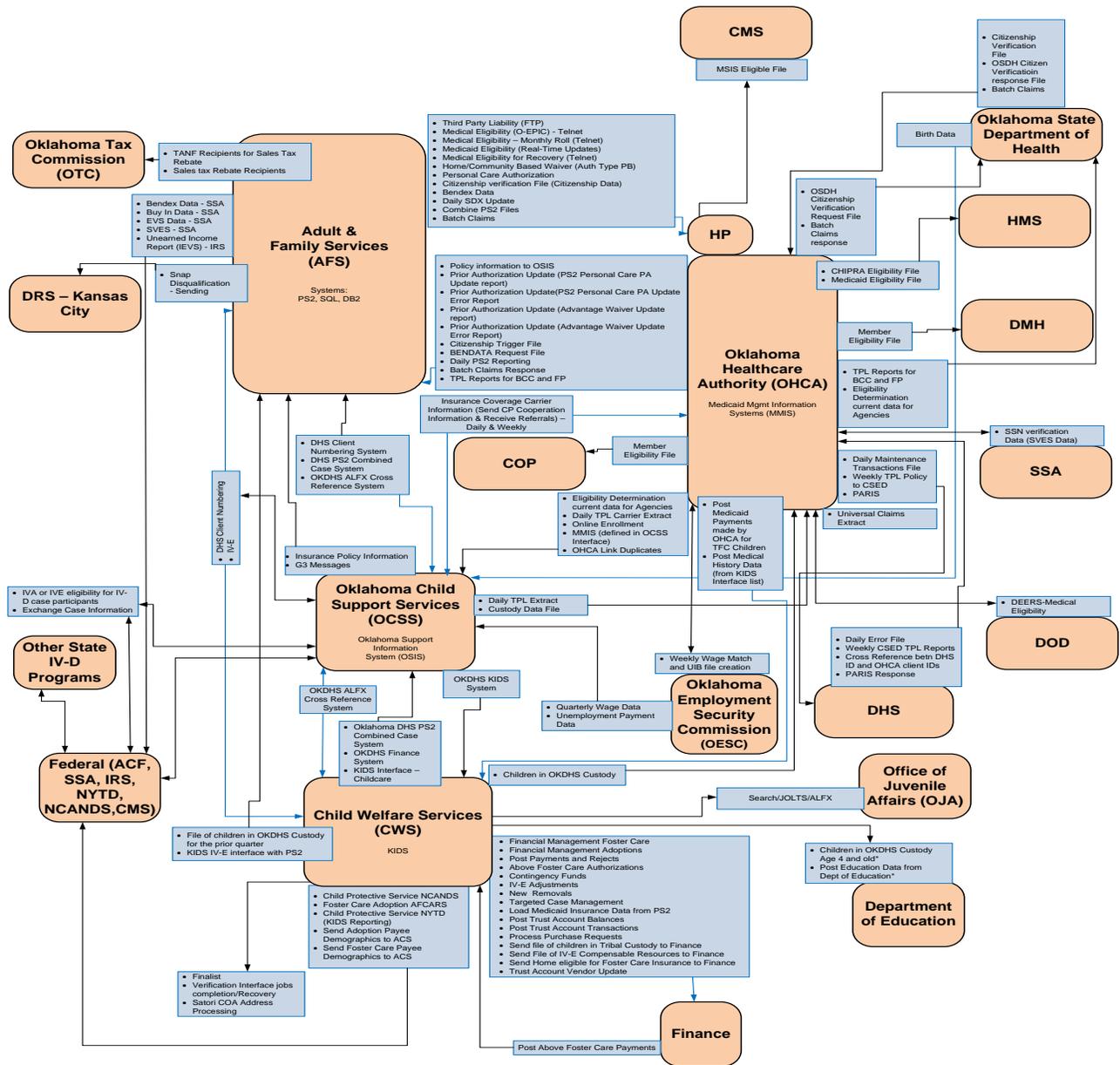


Figure A-1: AS-IS System Overview

The systems/owners identified in the Interoperability Project are shown in Table A-1 below. These systems have various types of data that are being exchanged via interfaces. Interfaces could be Real-Time (data is accessed directly any day/any time), Transactional or Transfer (push/pull via File Transfer Protocol (FTP) services).

Table A-1: Systems and Owners

System Name	Owner
Oklahoma Support Information System (OSIS)	Jim Hutchinson, Oklahoma Child Support Services (OCSS)
PS2	James Conway, Adult and Family Services (AFS)
KIDS	Carol Clabo, Child Welfare Service (CWS)
Medicaid Management Information System (MMIS)	Jerry Scherer, Oklahoma Health Care Authority (OHCA)
Vital Records	Kelly Baker, Oklahoma State Department of Health (OSDH)

See Appendix B-1 for a list of programs and services that each agency or division provides which requires an exchange of medical information.

Figure A-2 illustrates the AS-IS data exchanges among agencies with a focus on Eligibility and Enrollment.

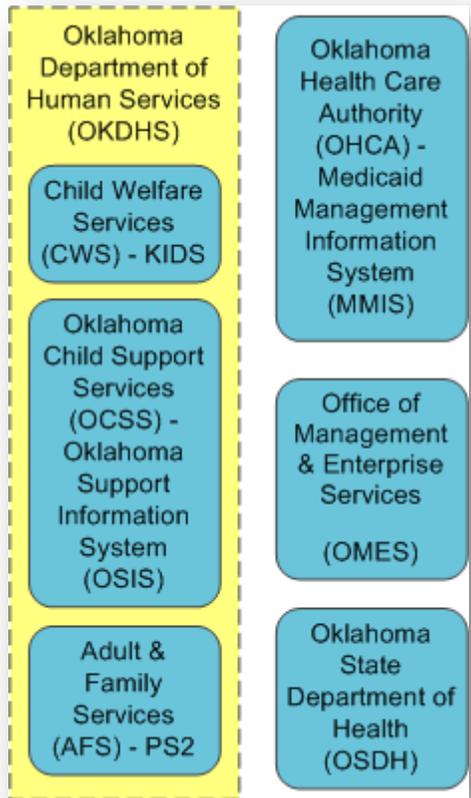


Figure A-2: AS-IS System Overview

6.1 Oklahoma Support Information System (OSIS)

OSIS is an automated system developed to assist OCSS in administering the state's Title IV-D of the Social Security Act program functions, including case initiation, case management, paternity and order establishment, cash and medical support enforcement, financial management, interstate case processing, locate, security and reporting. In addition to supporting the Oklahoma Title IV-D program, OSIS provides automation support to eight Tribal Title IV-D programs. The system currently processes over \$300 million in financial receipts and disbursements to child support consumers each year.

OSIS is specifically designed to comply with Title IV-D, associated rules and regulations published in the Code of Federal Regulations, the Office of Child Support Enforcement (OCSE) Systems Automation Guide, Oklahoma state laws, and policies of OKDHS. The system has been in continuous production operation since June 1991 and received federal compliance certification in August 2002.

Federal funding for OSIS and supporting staff is based on the Title IV-D Federal Financial Participation (FFP) matching rate established for OKDHS. OCSS submits funding requests annually to Administration for Children and Families (ACF)/OCSE via Operational Advance Planning document process and provides supporting program activity and expenditure reports OCSE-34A, OCSE-157 and OCSE-396.

The operational system is a COmmon Business-Oriented Language (COBOL) application using primarily IBM's Information Management System (IMS) hierarchical databases with some IBM's DB2. The system runs an IBM zEC10 mainframe with plans to migrate to a zEC12 platform in May 2013. The mainframe is fiber attached the data center Local Area Network (LAN) which is attached to the OKDHS' Internet Protocol (IP)-based Wide Area Network (WAN) servicing work locations statewide. Primary production data storage is an IBM DS8300 with an IBM TS7740 virtual tape system backup. Data backup is asynchronously mirrored to an offsite TS7740 for disaster recovery.

To access OSIS, users on the network initiate an IP based TN3270 connection from their desktop using Attachmate's EXTRA! Non-network system users may access OSIS through the internet with a Secure Socket Layer (SSL) Virtual Private Network (VPN) single user access session. Tribal programs may use the SSL VPN single user solution or may use a site-to-site VPN connection if local printing is desired. Access to specific OSIS functions within the system is controlled through rules defined in the Computer Associates' (CA) ACF2 security product. OCSS case participants may access OSIS case information through an Interactive Voice Response (IVR) system or through the Internet. Both methods use web services which directly access DB2 and access IMS data through IBMs' IMS Connect. Access to specific cases is controlled by the participant login ID. No update access is allowed.

OSIS is tightly integrated with several other applications sharing the OKDHS mainframe and will not function properly without the data shared among these applications. OSIS also supports dozens of interfaces to external partners. Tools including CyberFusion,

Connect: Direct and encrypted VPN tunnels are used to safely communicate with the external partners.

The following outlines OCSS's functional areas and the interfaces and partnership we have to carry out those functional areas of our program:

1. **Case Initiation:** Child support must receive a case referral or application for services to begin child support services. We obtain these applications from the general public by filling out the child support application for services which is sent to our State Case Registry for processing. OCSS obtains referrals through various electronic interfaces. For Title IV-E Foster Care, Temporary Assistance for Needy Families (TANF), child care, Non–Title IV-E and some Medicaid referrals, OCSS has an interface with AFS. For some Medicaid referrals, OCSS has an interface with OHCA. OCSS also receive referrals from our federal partners through our electronic Child Support Enforcement Network (CSENet) interface. Additionally, paper referrals for all other states, territories and foreign nations are mailed directly to our State Office Central Case Registry.
2. **Locate:** Once a child support case is established, services are provided to locate the non–custodial parent and certain assets. Types of activities included but are not limited to tracking their residence through an interface with a vendor representing the United State Postal Service (USPS), searching OKDHS records through our interface with the AFS PS2 system, checking driver's license records through our interface with the Department of Public Safety (DPS), checking many records from all other Title IV-D programs nationwide through our interface with the federal OCSE Federal Case Registry and checking employment information from the Oklahoma Employment Security Commission (OESC).
3. **Establishment & Paternity:** For married and separated cases, OCSS will establish a child support obligation through the local court systems. For cases requiring the establishment of paternity, OCSS offers services to conduct genetic testing of the case participants to gather scientific evidence on the probability of the father. The local court systems make the final determination of the legal responsibility of the father. This information is manually feed into the OSIS system.
4. **Enforcement:** When a non–custodial parent fails to honor a child support court order and is not making child support payments as instructed, the OCSS program and the automated system have many legal remedies available to compel the non–custodial parent make regular payments. Those legal remedies included but are not limited to credit bureau reporting by having an interface between OSIS and each credit bureau agency to report debt, Internal Revenue Service (IRS) and Oklahoma Tax Commission (OTC) interfaces that allow OSIS to intercept annual tax refunds, interfaces with national financial institutions (banks, credit unions, etc) to locate and intercept bank account assets, an interface with the OESC system to intercept unemployment benefits and the ability of OSIS to generate legal notices

to employers to deduct monthly child support payments from the non-custodial parents' pay check.

5. **Medical:** OCSS gets automated electronic referrals from AFS and OHCA for households that have been determined eligible to receive medical assistance. Most of these referrals receive the same activities as a case OCSS would receive through the application for service process. In addition OCSS collects cash medical "premium assistance" and reimburses the OHCA for some medical expenses. OCSS also works with the local court systems to obtain medical orders to ensure the children have medical insurance.
6. **Interstate:** All Title IV-D programs are required to accept and work cases from all other Title IV-D programs. As stated earlier OCSS receives both paper and electronic referrals from other Title IV-D entities. For the most part OCSS works these cases just like they would for an Oklahoma application for services.
7. **Finance:** The most technically complex part of the automated system and program is the financial component. Child support collections come in from all of the automated enforcement remedies mentioned above, directly from non-custodial parents, and from other states that collect on our behalf into the OCSS State Disbursement Unit (SDU). The SDU uses an electronic interface to transmit all payments received to OSIS for distribution processing. All payment exceptions are moved to a hold area and manually resolved by staff but the majority of payments are automatically issued to families through electronic interfaces with Xerox and Open System Technologies (OST). Within this financial area OCSS must submit federal reports like the OCSE-34A, OCSE-157 and OCSE-396 that tie to OCSS reimbursement and funding.
8. **Case Management:** OCSS staff manages the life of a child support case by handling specific activities like moving the cases from functional area to functional area as needed. They also adjust the court orders as situation change in the life of the custodial or non-custodial person. Court hearings and appointments are also managed in this functional area. If additional events occur that require the closing of a child support case, those heavily regulated closure reasons are documented here.
9. **Security & Reporting:** OSIS has special requirements in the area of security to ensure the data we collected is secure and safe and being viewed by the appropriate individuals. Security decisions are made by the OCSS program and then OMES security makes the physical changes to the access permissions. Reporting is critical for the OCSS program since program funding is dependent on it. The annual OCSE-157 and Oklahoma Advanced Planning Document (OAPD), and the quarterly OCSE-34A and OCSE-396 are what drive our funding for the program. OCSS use or interface with the AS400, Relational Database Service (RDS), Document Direct and WebFOCUS to support reporting needs.

Figure A-3 below depicts an overview of OCSS and AFS systems, specifically OSIS and PS2. This figure does not show all the interfaces between these systems but is provided for an overview.

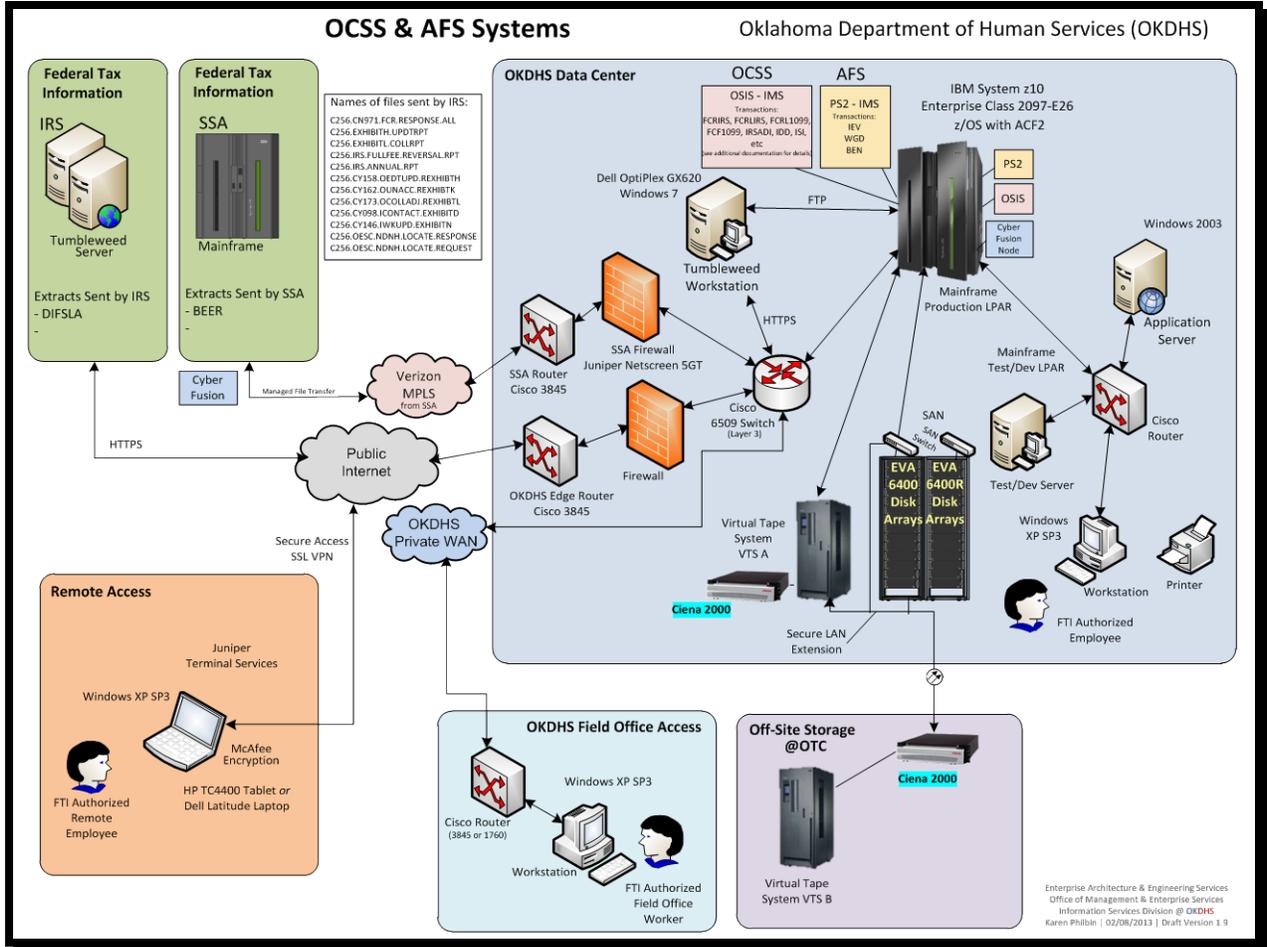


Figure 33: Overview of OCSS and AFS Systems

Figure A-4 illustrates the AS-IS Eligibility and Enrollment data exchanges for OCSS.

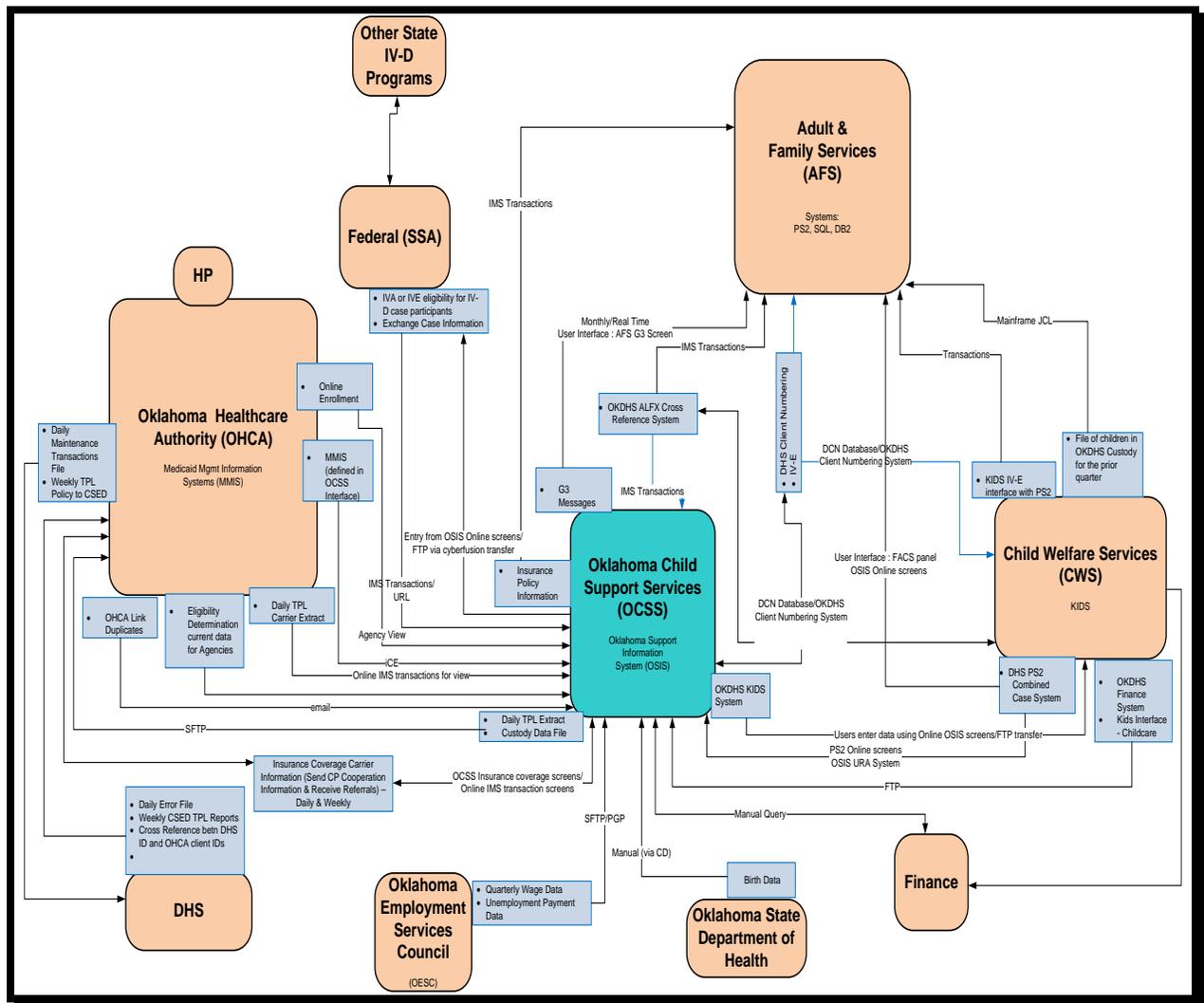


Figure 34: AS-IS Eligibility and Enrollment Interfaces for OCSS

6.2 PS2

The mission of AFS is to partner with stakeholders to ensure program and fiscal accountability by:

- Developing clear, concise policy for staff and providers
- Providing training for staff and providers
- Monitoring and evaluating service and benefit delivery

PS2 stands for “Payments and Services 2”. It is an arbitrary name given to the collection of databases, programs, transactions, modules, and functions that are directly related to AFS benefits and services. The PS2 system is a legacy system.

PS1/PS2 is the case information and data management system. It is a major client services system. It was developed in 1981 to help AFS and Developmental Disabilities Services Division (DDSD) serve the needs of the people of Oklahoma.

The backbone of the PS2 system is a series of IMS databases. These databases are called “hierarchical databases”. Most new systems rely on “relational databases”.

Some of the primary tables in PS2 are:

- CA221DBD – PS2 Cases Sections A, B, C, D, E, and F
- Primary Segment – What case looks like with pending updates applied
- First History Segment – Case section after updates have cleared edits and case has updated
- CA244DBD – Holding place for pending updates to PS2 case Sections A, B, C, D, E, and F
- CA251DBD – Notices
- CA908DBD – Authorizations (Section K)
- CC144DBD – CWA Database
- CB250DBD – AP Info (Section I)
- CB600DBD – Medical (What is sent to EDS)
- CB800DBD – History (Sections A, B, C, D, E, and F)
- CL001DBD – Client Number (Primary)
- CL146DBD – Client Number (History)
- TL022DBD – Third Party Liability (TPL) (Section H)
- WA481DBD – Providers

Case numbers generated by the Case Number Assignment System provides the primary key to facilitate non-redundant collection, maintenance, and use of basic client data for AFS and DDSD services and a critical interface for OCSS. It performs eligibility for:

- SNAP
- TANF
- Child Care
- Title II and XVI
- Medicaid
- Medicaid Home and Community Based Waivers Energy Assistance
- Title V programs

It contains services related information as it relates to the client’s health and welfare for the following divisions: AFS, OCSS and DDSD. This is a 24/7 system which includes:

- Applications for processing case number assignment
- General client demographic
- Financial and family assistance
- Food Nutrition

- Medical eligibility and services
- Authorizations
- Day care services
- TPL information
- Data exchange
- Energy services and supported data

It contains the following subsystems:

- **Authorizations:** A data collection, validation, storage, and reporting system for establishing records about authorizations for Department expenditures for certified clients.
- **Case Number Assignment:** Online transactional system which generates case numbers for client information for OKDHS clients.
- **Case Certification:** Provides the processes for data collection, validation, storage, and eligibility determination.
- **Case Management and Reporting:** Online and batch system for reporting case information, statistical reports, and sending report files to meet Federal, State, and administrative requirements.
- **Developmental Disability Case Update:** Case benefit tracking system for people receiving disability services.
- **Data Exchange:** Online and batch file processing system from which OKDHS performs information data exchanges with Federal partners and other entities.
- **Electronic Payment Systems (EPS) (Electronic Benefits Transfer (EBT), Electronic Child Care (ECC) & Electronic Payment Card (EPC)):** Process to electronically transfer financial benefits, SNAP benefits and child care authorizations to clients and provides them via debit cards.
- **Family Assistance:** Disabilities assistance program is a cash payment program for families who are caring for children under age 18 at home.
- **Financial Activities:** Maintains on-line five years of case food benefit and warrant issuance information; provides on-line inquiries for this information; provides the vehicle for re-issuing documents which have been returned; provides for supplemental issuance; and provides for recording of reconciliation information.
- **Future Actions:** Provides for the storing and executing of transactions on a preset date and time.
- **Low-Income Home Energy Assistance Program (LIHEAP):** This program is to provide assistance to eligible households to meet the costs of home energy that are excessive in relation to household income.
- **Notices:** This maintains all relative information about all notification letters (notices) which are related to a case and sent to clients and/or vendors.
- **Level of Care and Plan of Care:** Determines the level of care a client needs so that a plan of care may be developed for people with Developmental Disabilities. This is Medicaid and home community based waivers.

- **Non-Federal Medical and Supported Living:** Non-federal medical authorization and payment system for medical services and supported living authorizations and record keeping for developmental disabilities.
- **Supported Data and Application Repository:** The online validity data, descriptive data, and systems documentation. It contains documentation and parameters associated about any entity that needs system wide availability for people or application use.

6.2.1 Family Assistance and Client Services (FACS)

FACS is the software used by OKDHS staff to update and maintain AFS case information. FACS is a “front end” to the PS2 System. The primary purpose of the FACS software is to gather information, send it to PS2 (through a clone of the ff transaction called fu) or DB2 as appropriate and display a response from PS2 and DB2. Other features in FACS include Case Notes, Case Status Monitoring, and Notice Generation. It provides a Graphical User Interface (GUI) which allows the user to navigate through tabs designed to follow the flow of an applicant interview. Through this GUI the user can enter information through “free form” fields, check boxes, or select options from drop-down fields. This is considered to be an improvement over entering the information on the PS2 “green screens”, which required the user to follow a strict format and required that the user knew the PS2 codes values, as opposed to selecting a description from a drop-down field.

FACS is written in Sybase’s PowerBuilder. The first version of FACS went to production in December, 1996. The software is now considered to be a legacy application. FACS is a client/server based application (which means that it runs from the local county office server) as opposed to a web based application (which would run using web technology from one central site). Most new generation software development is done with web based software (such as .NET or C# (C Sharp)).

Figure A-5 illustrates the AS-IS Eligibility and Enrollment data exchanges for AFS.

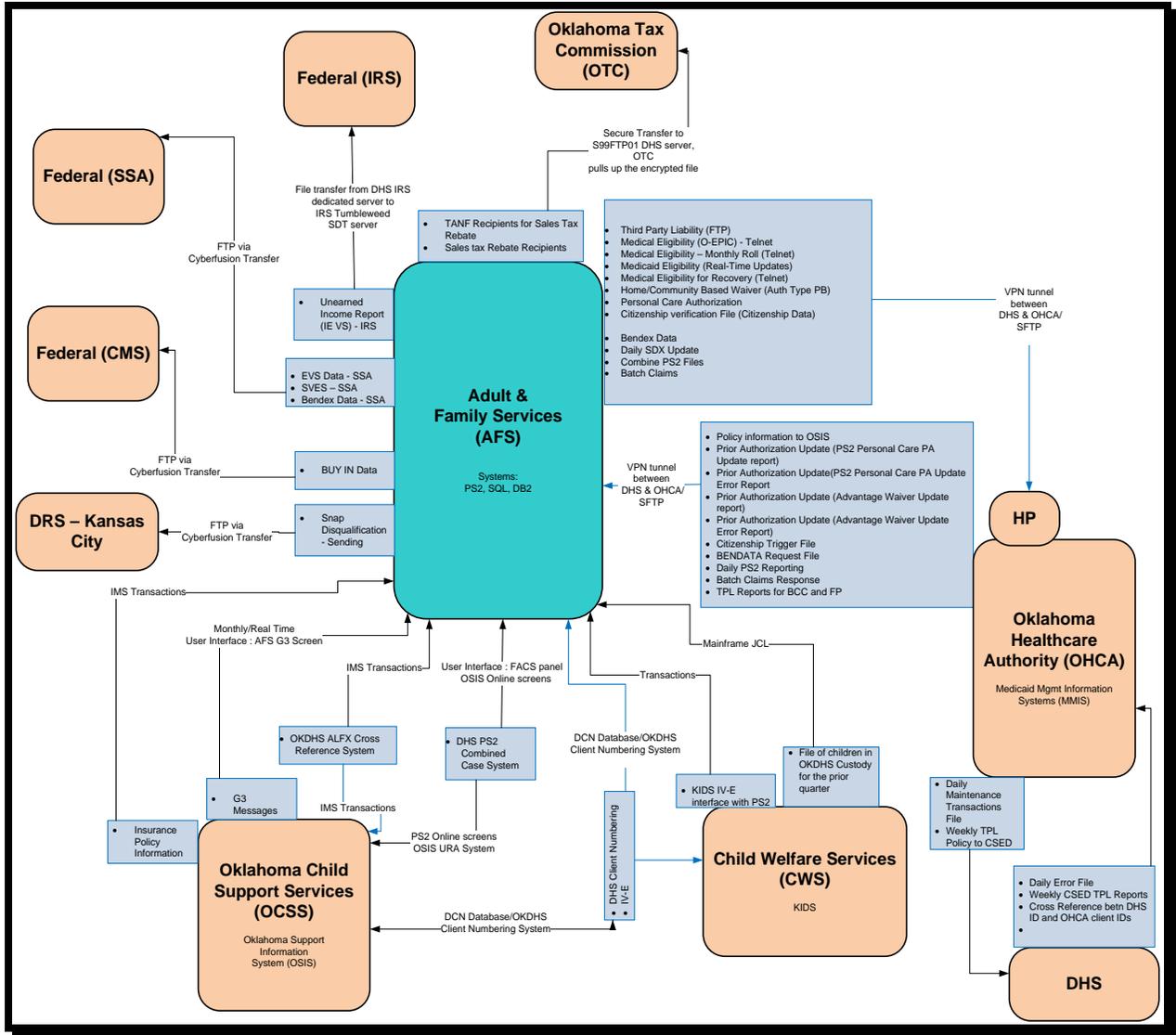


Figure 35: AS-IS Eligibility and Enrollment Interfaces for AFS

6.3 KIDS

OKDHS CWS was the first state in the nation to implement a comprehensive Statewide Automated Child Welfare Information Systems (SACWIS). SACWIS is a comprehensive automated case management tool that supports social workers in foster care and adoptions case management. SACWIS is intended to hold the State’s “official case record”, which is a complete, current, accurate and unified case management history on all children and families served by the Title IV-B/IV-E State agency. The software application was created in 1994 and deployed statewide to the field in May 1995. The acronym for the Case Information and Data System (CIDS) was aptly changed to KIDS. KIDS is a Windows based two-tier client server application with the front end using Sybase’s PowerBuilder 11.5 and the back end database using Oracle 10g. The newest

release of the application is stored on a server in the local Child Welfare Services (CWS) offices, and CWS staff uses a desktop client to connect to this database to run the application. Information/data entered into the KIDS system is not stored on the endpoint device or the local office server; it is stored in a central Oracle database at OMES. The instance of the application runs on an endpoint device connected to a single large database via a WAN. Remote access to the system can be achieved through a server farm via a web based portal. It provides essential support to the CWS in their mission of improving the safety, permanency and well-being of children and families involved in the Child Welfare system. The KIDS application uses Global Name Recognition (GNR) for name search. The system is tightly integrated in the operations of CWS. The statewide hotline uses the system for logging calls, and distribution to local offices. Investigation and Permanency Planning documentation is all entered into and retained in the system, and is used in court for case presentation.

eKIDS is a Windows based web enabled subset of the KIDS Application developed with Active Server Pages (ASP), JavaScript, VBScript, HyperText Markup Language (HTML), Cascading Style Sheets (CSS) and SQL (Structured Query Language) using an Oracle database. It allows online access of selected Child Welfare information to CWS partners. These partners include Native American tribes, Oklahoma Children's Services (OCS) contractors and liaisons, court officials: judges and district attorneys, school-based social workers, and child support enforcement personnel.

KIDS Application Help Desk (KAHD) is a Windows based two-tier client server Help Desk support application with the front end using Sybase's PowerBuilder and the back end database using Oracle. The KAHD application is used as an incident and response tracking system and also supports software development life cycle for the KIDS application support team. Apart from tracking problems, it logs client requests and/or enhancements to the KIDS application. The KAHD application is available to the KIDS Technology and Governance and the KIDS development teams providing an organized method for documenting and reviewing the KIDS application as to: Operational anomalies, application enhancement requests, KAHD's associated with an identified screen, and all KAHD's associated with a specified business function.

Data is pulled from the following systems to provide enrollment authorization for services and payments:

- AFS electronic records (IMS & FACS)
- OCSS
- OHCA medical histories of custody children
- Social Security Administration (SSA) (Supplemental Security Income (SSI) & SSA financial information)
- OKDHS Finance Office (payments for foster care/placements)
- Office of Juvenile Affairs' Juvenile On-Line Tracking System (JOLTS) which tracks juvenile criminal histories
- Multiple day care providers throughout Oklahoma

There are multiple and varied external consumers for the data maintained in the KIDS database. Data is used for ad hoc and state reporting. The most important external consumer of CWS data is the federal government. A crucial function of KIDS, other than a mechanism of facilitating service delivery to CWS clientele, is the federally mandated reporting of:

- Adoption and Foster Care Analysis and Reporting System (AFCARS)
- National Child Abuse and Neglect Data System (NCANDS)
- Reporting of case worker visitation data
- National Youth in Transition Database (NYTD)
- Reporting of Children and Family Service Reviews (CFSR) data

The Children's Bureau (CB) Under ACF supports the development of state and tribal child welfare reporting systems to enable the collection and analysis of important information about children and families, as well as improve case practice and management.

The CB supports the development of state and tribal child welfare reporting systems to enable the collection and analysis of important information about children and families, as well as improve case practice and management.

- **AFCARS** on all children in foster care and those who have been adopted with Title IV-E agency involvement. Title IV-E agencies are required to submit AFCARS data twice a year.
- **NCANDS** is a voluntary data collection system that gathers information from all 50 states, the Washington, D.C., and Puerto Rico about reports of child abuse and neglect.
- **NYTD** collects information about youth in foster care, including outcomes for those who have aged out of foster care. This data is collected, validated and transmitted periodically to the CB on a routine scheduled basis.

In addition, there are additional "audits" performed on a periodic basis varying from annually to every few years. These audits include a Title IV-E Financial Review. The purpose of this review is to assess payment accuracy through an examination of case record documentation (both physical and electronic case files). Another audit is the CFSR which enables the CB to ensure conformity with Federal child welfare requirements, to gauge the experiences of children, youth, and families receiving State child welfare services, and to assist States as they enhance their capacity to help families achieve positive outcomes.

The following resources provide results and lessons learned from the CFSR's and address the implementation of the CFSR process in the United States:

- Key external partners of CWS have special access to CWS Data and may also be important data creators who input data into the system directly. CWS contracts for

Prevention/Family Centered Services, Reunification, Parent Aide, and Resource Home Maintenance services with outside social service agencies throughout the state. These contractors are called OCS contractors. They have access to the KIDS database via web based application called “eKIDS” (ASP.NET Passport). OCS contract workers log into the system via the internet and have access to limited data and can enter documentation of their case work activities directly into the KIDS database via eKIDS. Native American tribal workers also have the ability to enter limited case documentation of their activities via eKIDS.

- There are other community external partners who also have more direct and timely access to KIDS data via eKIDS (ASP). This system is separate from the one used by OCS contractors and less complex being limited to structure “Read only” capacities. They do not have the ability to enter data into the system. These external partners include Juvenile Judges, District Attorneys, School Based Social Workers, and Post Adjudication Review Board (PARB) members.
- There are multiple additional external parties that can have access to CWS data on a prearranged or ad hoc basis. They include the previously mentioned CB entities (CFSR, Title IV-E Audits, AFCARS, NCANDS, and NYTD). Universities, colleges, schools and researchers from public or private agencies can request data and receive it via various types of electronic means if there is an approved data sharing agreement. Various reports are available to the legislature, students, general public, and the Pinnacle Plan Co-Neutrals (monitors of a federal lawsuit settlement agreement).
- There are multiple internal customers of CWS data. CWS Specialists and other members of CWS Management and Support utilize multiple reports to help maintain data accuracy and monitor case progress and case management efficacy.
- CWS Workers/Personnel: CWS Specialists, Program Field Representatives, District Directors, Field Analysts, Programs Supervisors, Program Managers, Deputy Directors, Administrative Technicians, Administrative Assistants, and Secretaries, County Directors. The work performed by CWS Workers/Personnel involve CWS Intake, CWS Investigation, Permanency Planning, Foster Care/Bridge, Adoption, Adoption Subsidy, Guardianship Subsidy, etc.
- Other sister divisions in OKDHS have workers crucial to the delivery of CWS services. They include: Social Service Specialists, Departmental Disabilities Services Division (DDSD) Case Managers, Child Care Licensing Specialists, Child Support Specialists, Social Service Inspectors, and Adult Protective Services Specialists. Some of the CWS related work they perform includes Foster Care Payments, Child Support, and Paternity Determination, Title IV-E Eligibility Determination, Medical Eligibility Determination, TANF, SNAP, Day Care Eligibility and Authorization, and DDSD services, etc.

The information (data) contained within KIDS database can only get there via manual data entry by CWS Specialists/Personnel or specific other external partners via limited direct entry or periodic data exchanges into the KIDS database. Only CWS Specialists (All CWS Personnel), Title IV-E Custody Specialists, and OCS contractors have direct access to the KIDS software application and enter data directly via the KIDS Application. Data transfers are via electronic “data packets” that are updated on a varying schedule (Real time, hourly, daily, weekly, monthly).

Figure A-6 provides a high level overview of the KIDS Application Architecture.

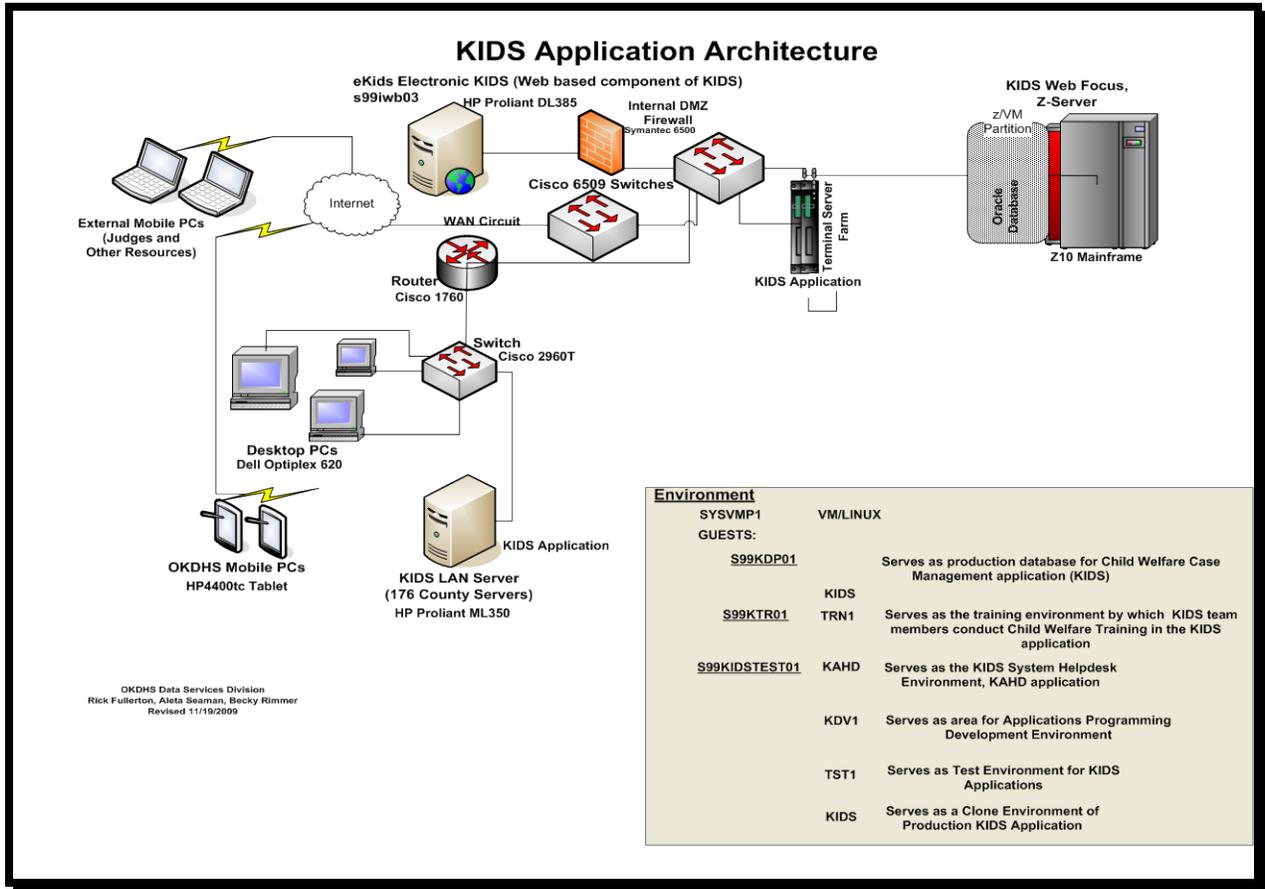


Figure A-6: KIDS Application Architecture

Figure A-7 illustrates a functional view for KIDS

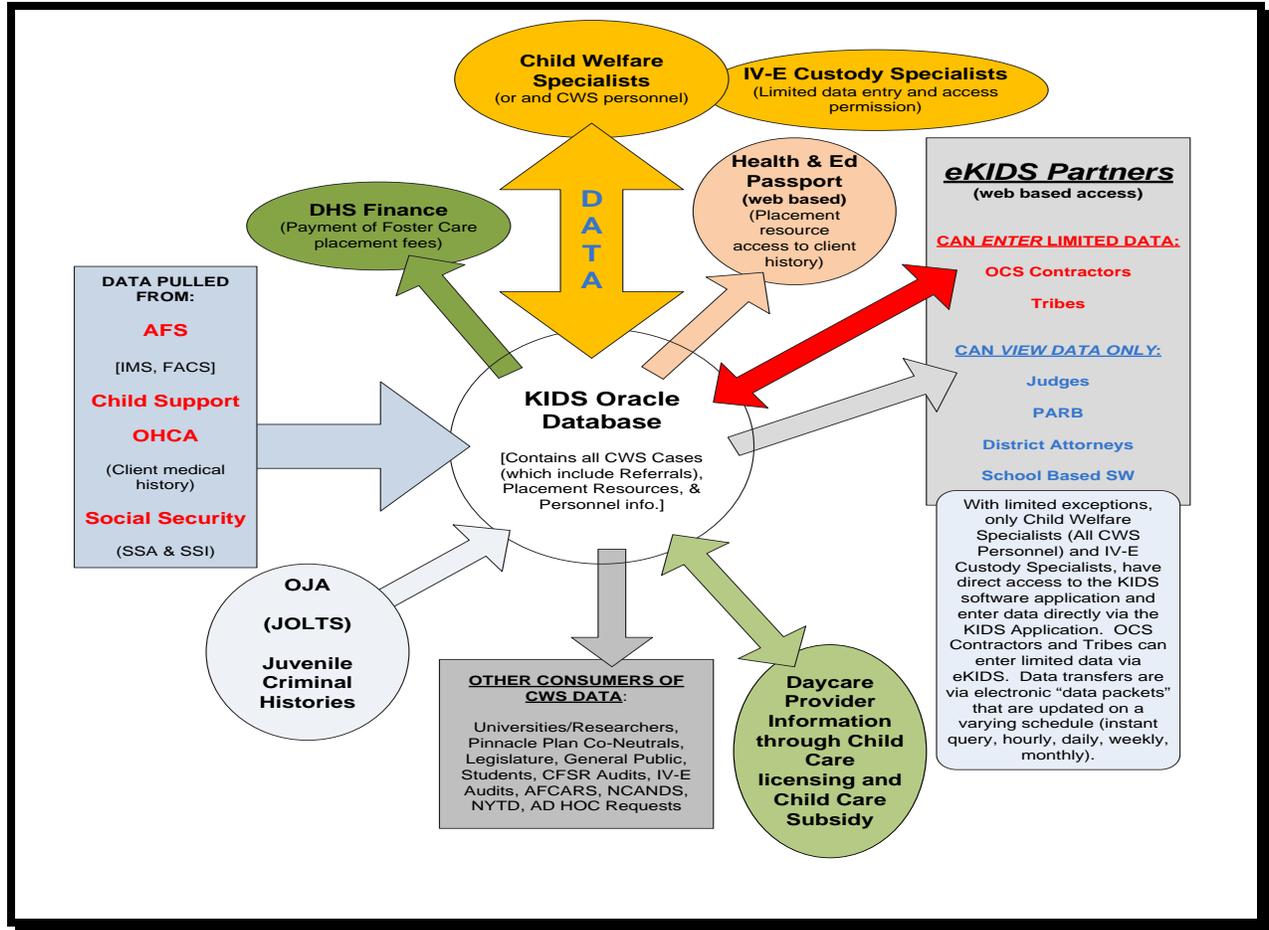


Figure A-7: KIDS System

Figure A-8 illustrates the AS-IS Eligibility and Enrollment data exchanges for CWS

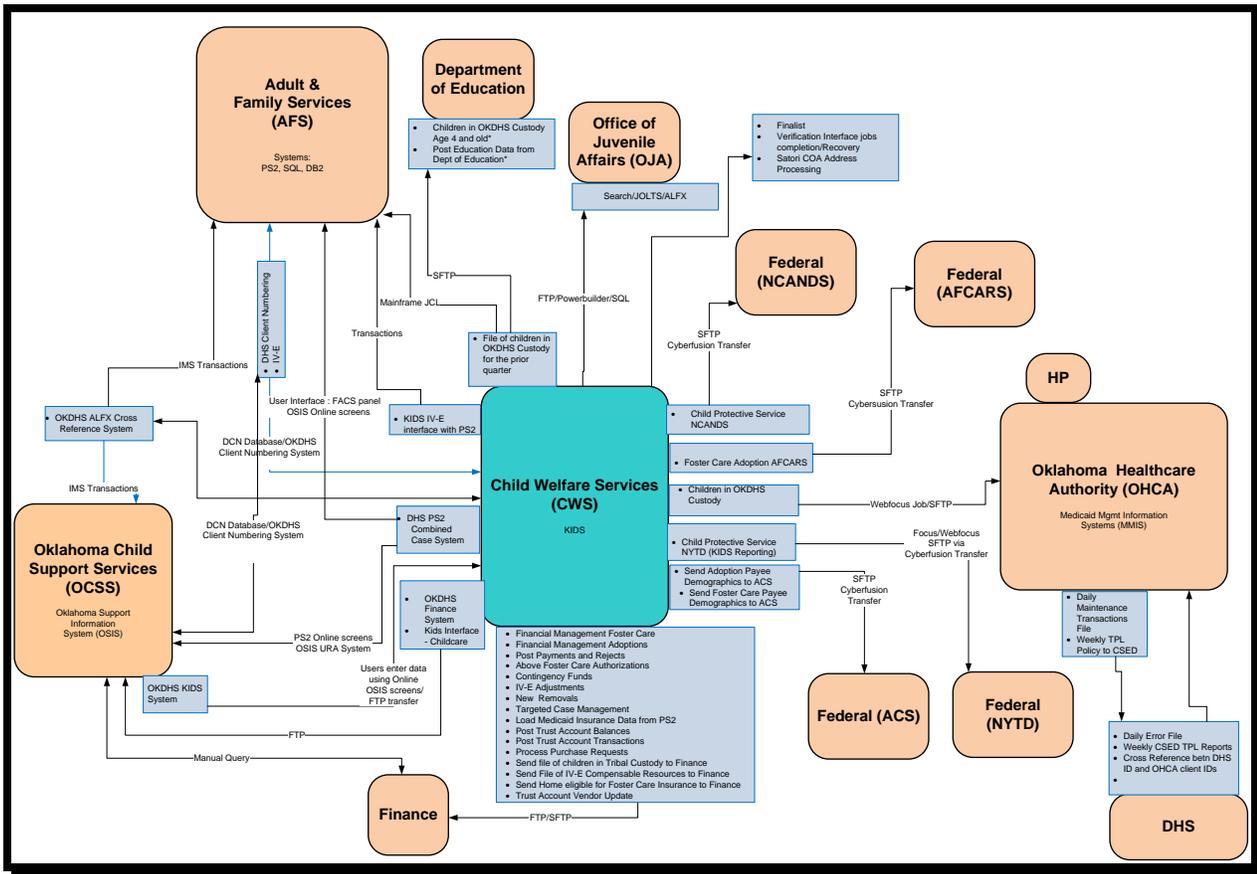


Figure A-836: AS-IS Eligibility and Enrollment Interfaces for CWS

6.4 Medicaid Management Information System (MMIS)

Title XIX of the Social Security Act is a Federal/State entitlement program that pays for medical assistance for certain individuals and families with low incomes and resources. This program, known as Medicaid, became law in 1965 as a cooperative venture jointly funded by the Federal and State governments (including the Washington, D.C. and the territories) to assist states in furnishing medical assistance to eligible needy persons.

The MMIS was developed by Hewlett Packard Enterprise Services (HPES) to serve the needs of the federally mandated program for all states. It is Healthcare Financing Administration (HCFA) certified and has been operational since 1995. MMIS is a highly sophisticated, feature-rich system centered on a strong, Medicaid-specific relational data model. It divides the application into components which may be processed on multiple networked computers. This design and supporting architecture deliver enhanced flexibility, scalability, and reliability, as recognized by the National Association of State Information Resource Executives (NASIRE) Award for innovative use of technology that

the system received after its implementation in the State of Indiana. The systems architecture is Medicaid Information Technology Architecture (MITA) compliant and is enabled to support a Service Oriented Architecture (SOA).

The storage area network (SAN) design allows improved usage, and rapid provisioning of space to whatever application is needed. The SAN devices are consolidated units with redundancies built in for high availability. Experience has shown that SAN devices provide more efficient use of space and the device can be managed from a single console. A second SAN unit will act as a geographically dispersed electronic vault site creating a much faster disaster recovery response.

Referring to the Figure 9 below, the system is logically divided into three primary components:

- Claim Engine is responsible for receiving interactive transactions from external sources, adjudicating them, and returning the appropriate response.
- Online/Batch Application is responsible for maintaining and reporting on data contained within the online database.
- History and Back-End reporting component is responsible for analyzing, reporting, and supporting the management of the activities that have occurred in the two front-end systems.

The external interfaces describe a variety of data sources which influence processing within the system. The External Data Submission Entities are organizations that supply information to the MMIS. PS/2 is the primary source of recipient eligibility information. HCFA is a federal organization that supplies many different types of data feeds.

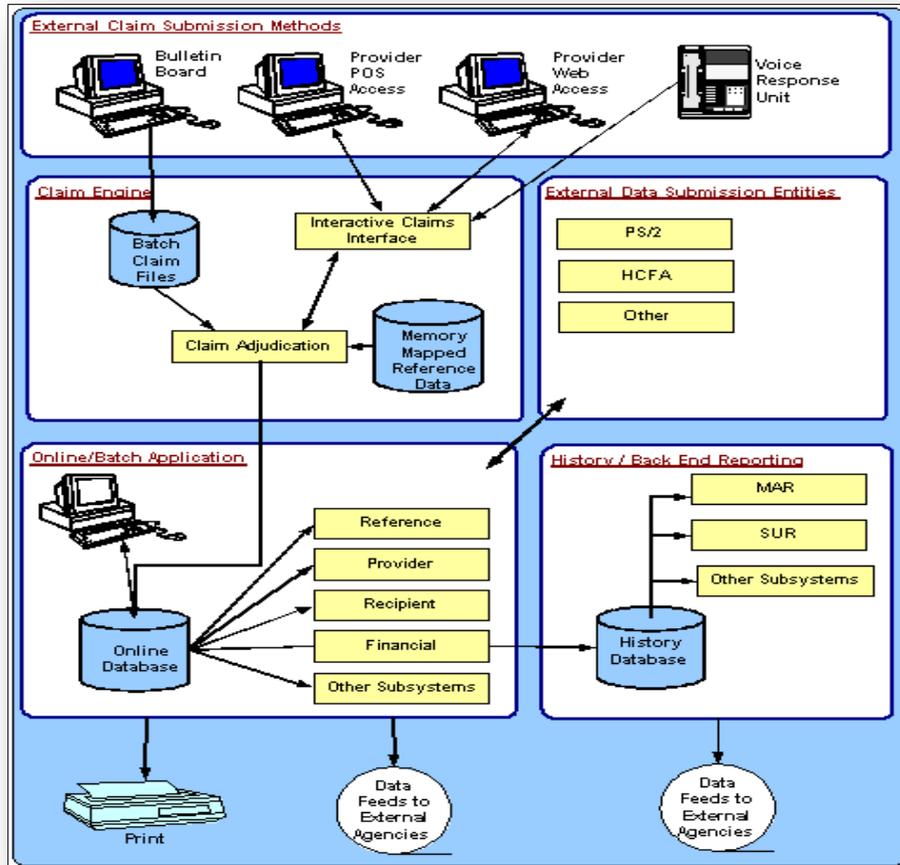


Figure A-9: MMIS Logical Components

MMIS physical infrastructure includes high-bandwidth network components, industry-leading security, and full redundancy in support of the primary user groups:

- OHCA
- External stakeholders
- HPES operations
- HPES account staff

Traffic across the network is managed by a series of switches, firewalls, and routers that are interconnected by 10 GB fiber interfaces. Primary entry points to the systems include direct local connections (for onsite staff), dedicated VPN tunnels (for remote staff and external trading partners), the Internet, and the newly implemented HP Healthcare Network Cloud (HNC). The HNC is a private, fully secure, national network that provides Electronic Data Interchange (EDI) and intranet connectivity between OHCA and national HPES Healthcare and Business Process Outsourcing (BPO) sites. The internet connection is the primary entry point for providers, other state agencies, and provider representatives.

The Oklahoma MMIS physical infrastructure also includes new UNIX and Windows servers and supporting systems upon which MMIS now processes. Physical devices, operating systems, server software, Database Management Systems (DBMS's), utilities, and applications have all been upgraded to high-end, expandable versions. The infrastructure has been virtualized for service stability and ease of maintenance. Components reside in HP's Blade System c7000 enclosures, which provide all the power, cooling, and Input/Output infrastructure needed to support modular server, interconnect, and storage components for the next several years.

Figure A-10 depicts OHCA's MMIS current AS-IS architecture.

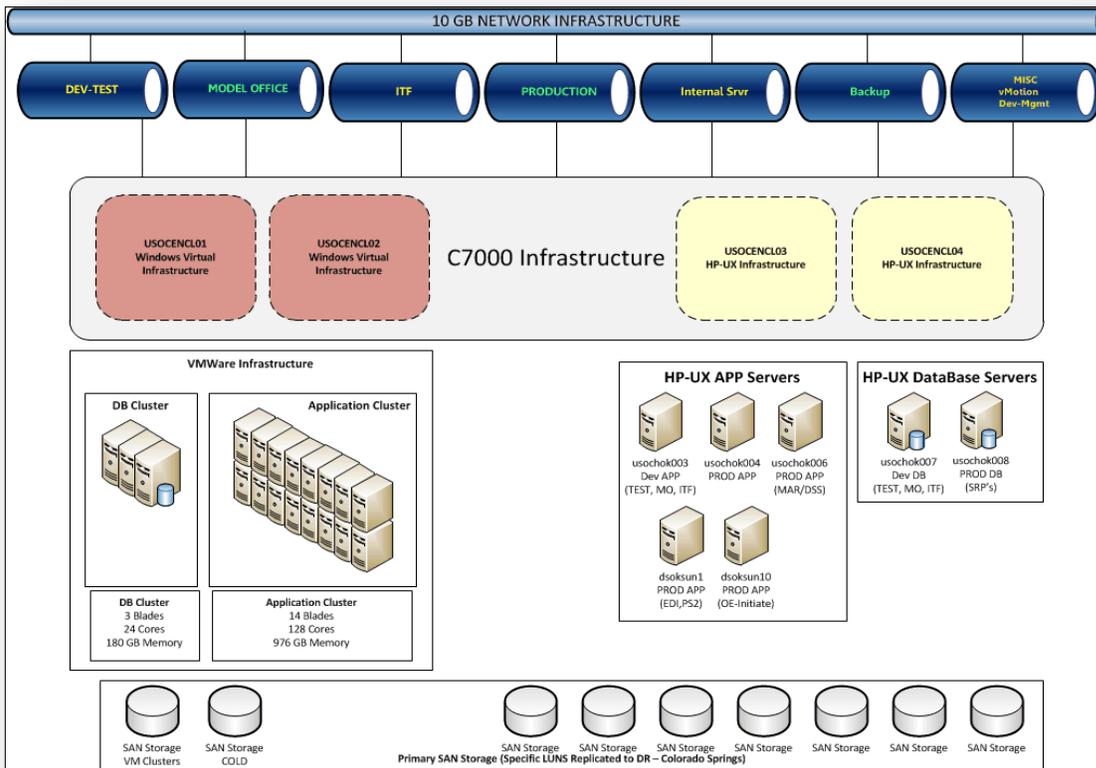


Figure A-10: MMIS Architecture

Figure A-11 provide an AS-IS Eligibility Determination Functional View for OHCA. While Figure A-12 illustrates the AS-IS Eligibility and Enrollment data exchanges for OHCA.

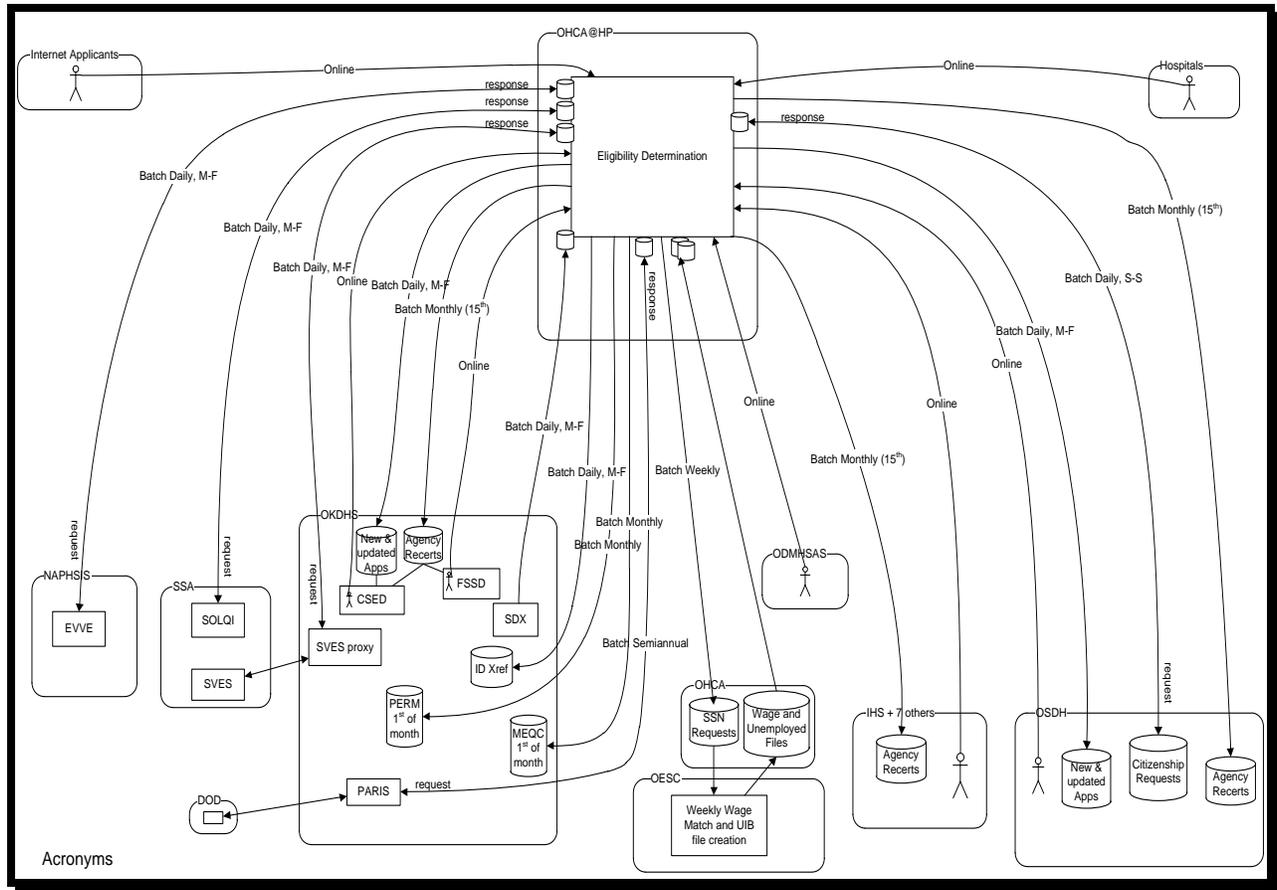


Figure A-11: AS-IS Eligibility Determination Functional View for OHCA

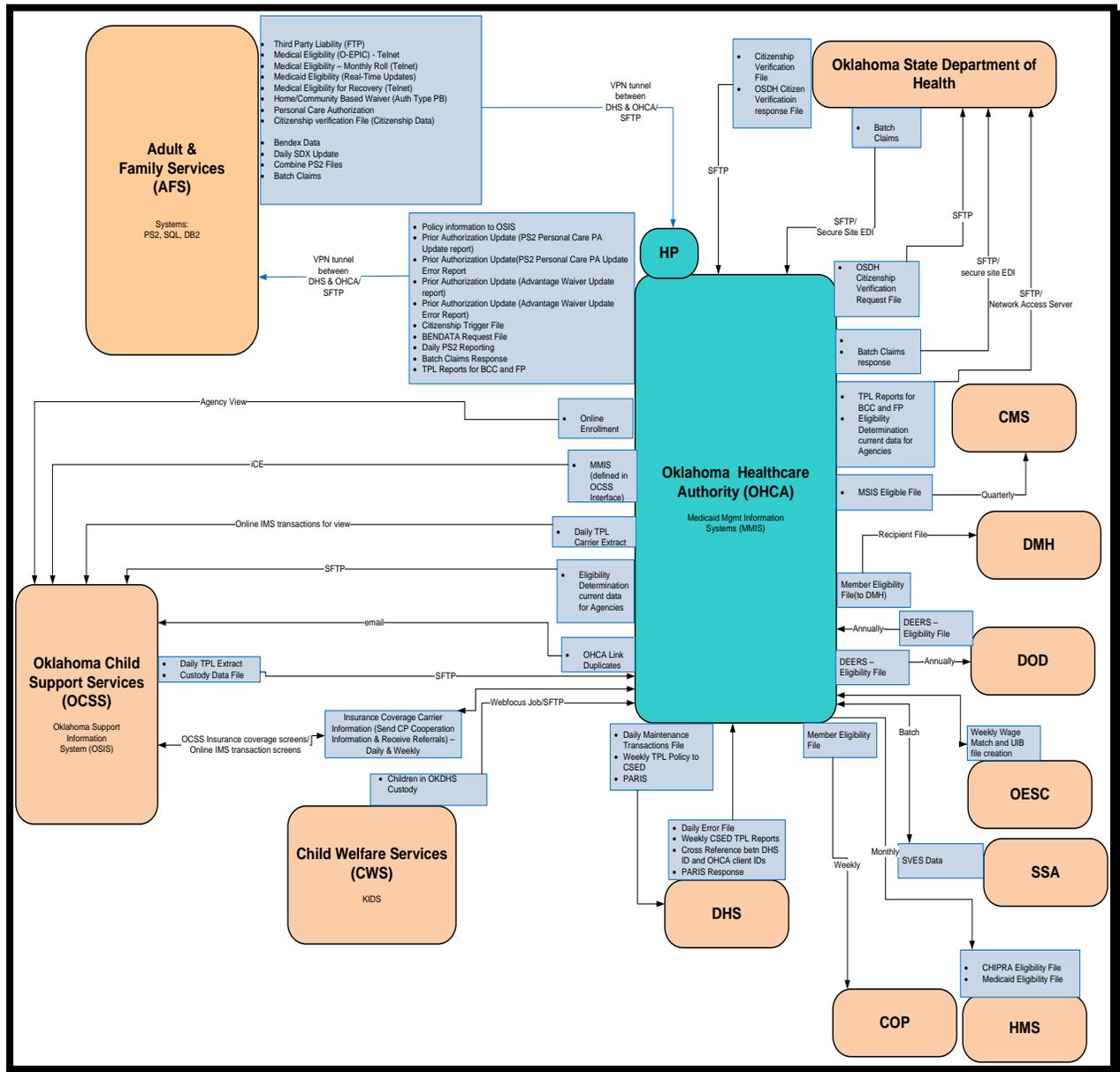


Figure A-12: AS-IS Eligibility and Enrollment Interfaces for OHCA

6.5 Oklahoma State Department of Health (OSDH)

Most of the systems at OSDH were independently designed, developed, and are uniquely customized to the particular program. The bulk of OSDH's systems are designed for capturing, tracking, and reporting information, and mostly for non-clinical purposes. A few are used in providing both clinical and non-clinical services. The most common business processes supported by OSDH systems are data capture/collection, data management, data analysis, tracking, and data reporting. Some systems additionally support limited case management functions, threshold identification, and notification/letter generation,

primarily to providers. Where Centers for Disease Control and Prevention (CDC) developed systems are being used, there is little commonality of platform, format, or content across systems. OSDH is working to migrate some of the systems to a standard SQL-based platform and integrate them into OSDH's Public Health Oklahoma Client Information System (PHOCIS), which supports client services at the county level and allows these external users to directly and more effectively access and use the data. All of the systems supporting direct client services have been migrated into PHOCIS. Few systems have direct interfaces that allow data to be sent/received between systems with no human intervention. Of the small numbers that are automated, only a few are set up to utilize Health Level 7 (HL7) formats.

Figure 45 provides a functional look at the OSDH Vital Records, Birth Registration Workflow. Birth information to OCSS – It is the interface where birth information is sent to OCSS with Personal Identification Information (PII) removed. The file is kept at an File Transfer Protocol (FTP) site for pickup by OKDHS.

Birth data cannot be used for Master Person Index (MPI) purposes in the Enterprise Service Bus (ESB) because there's a state mandate that allows the sharing of such information only for certain purposes as defined in the mandate. Since it is a State mandate even sharing this data with security in place would be against the law.

The Vital Records for a birth has a Birth Certificate Number and a Record Number attached to it but it is internal to the system. The Death System has a different unique identifier. The Record Number and Birth Certificate Number is not a unique identifier that is used throughout the systems. It is only applicable to the Birth System, see Figure A-13.

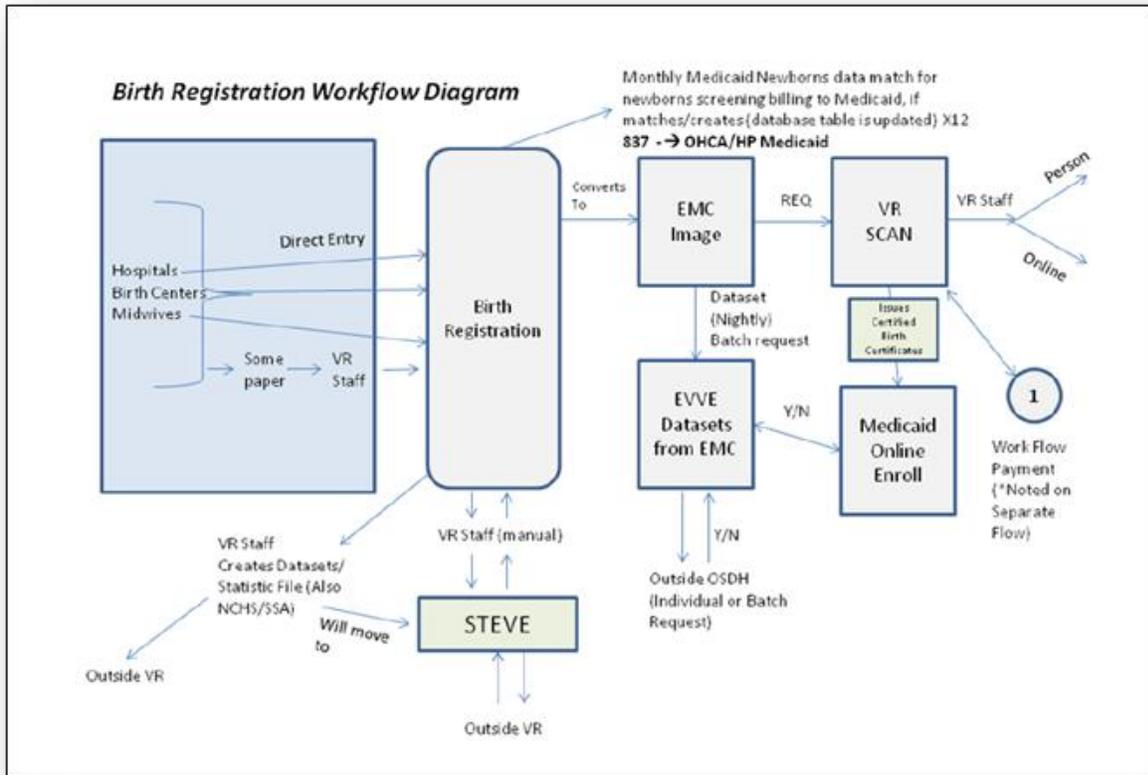


Figure A-13: OSDH – Vital Records, Birth Registration Workflow

6.5.1 No Wrong Door (NWD)

Software needed for OSDH to interface with the No Wrong Door (NWD) Project. This allows PHOCIS access/presentation of SoonerCare application forms hosted on remote servers. PHOCIS is able to create new SoonerCare applications and also maintenance of existing applications. OSDH also regularly receives and stores new/changed SoonerCare applications.

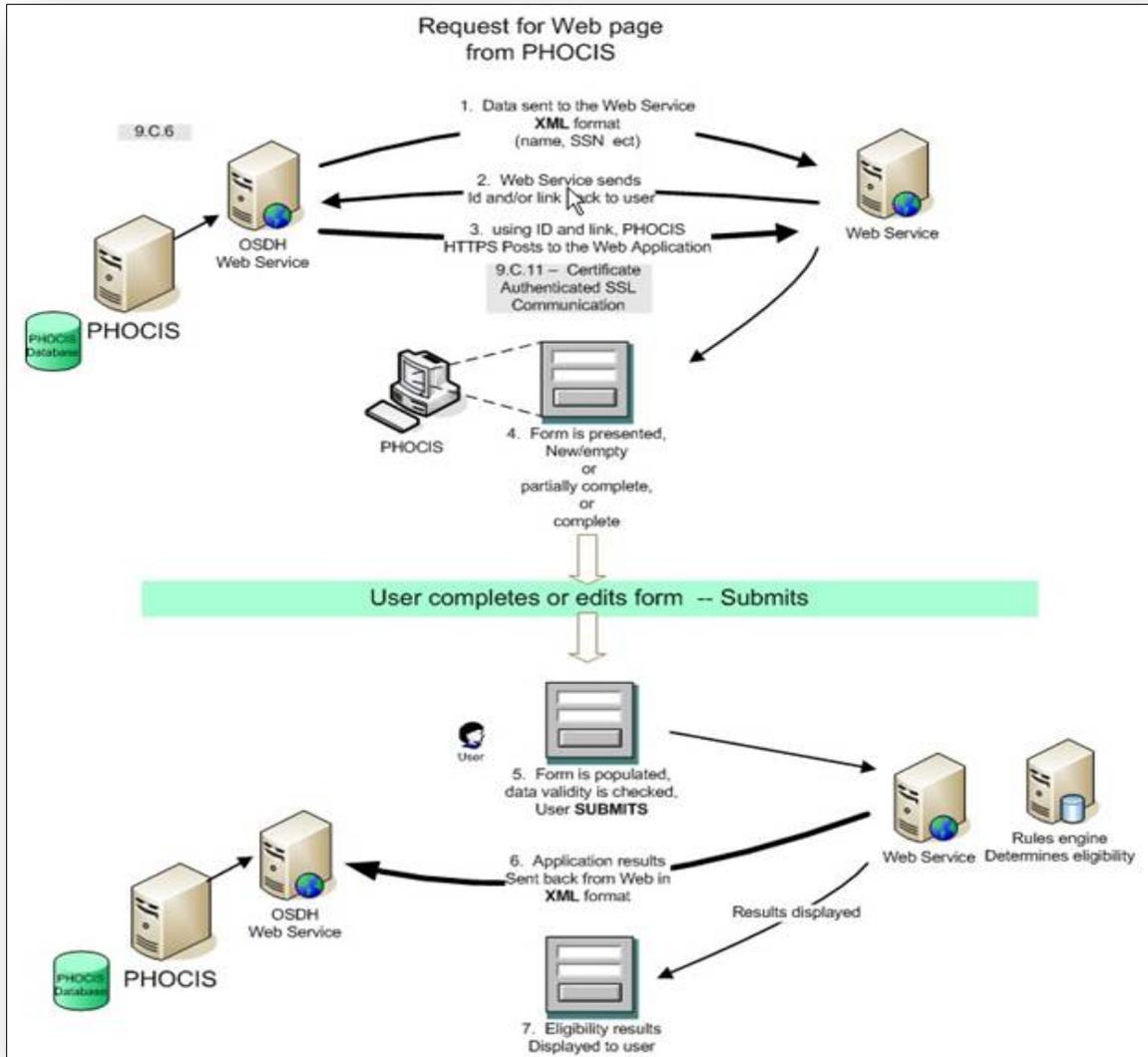


Figure 37: PHOCIS

PHOCIS makes a request from OHCA’s (HPES) web service for a new or existing SoonerCare application. Extensible Markup Language (XML) data is sent from PHOCIS to request a SoonerCare application, Figure A-14 above. This data contains any demographic data OSDH may have for that the person. Also, if an Application Tracking Number (ATN) exists for the person, OSDH sends it. Demographics data from OSDH is used by OHCA’s (HPES) to partially complete new applications.

OHCA’s (HPES) web service returns to the PHOCIS web service an “ATN” and a URL/link which is used by the PHOCIS web service to make an HTTPS “Post” call to the OHCA’s (HPES) web service. If it is a new application, OHCA’s (HPES) returns a new ATN when the web page is requested.

The PHOCIS application presents/displays the editable SoonerCare application.

PHOCIS does not have “control” of the functionality/workings of the SoonerCare application form displayed; PHOCIS merely presents the interactive web page served by the OHCA’s (HPES) web service.

PHOCIS users complete the SoonerCare application and submit it.

Once a completed SoonerCare application is submitted by the user, OHCA’s (HPES) web service returns to OSDH an XML file containing the contents of the SoonerCare application. Only completed applications are sent to OSDH.

For each application approved/changed, the SoonerCare application is sent to OSDH from the OHCA’s (HPES) web service(s). These transmissions occur in real-time. The record sent contains all of the agency fields as well as the OHCA determined data. OSDH stores these in the OSDH-NWD database by inserting new applications or updating existing applications:

- Citizen verification – batch data exchange
- Batch data exchange between OSDH and OHCA of data to verify citizenship.
- OHCA sends a file requesting checks to be made. OSDH returns a file of results.
- Nightly process, 7 days a week

Figure A-15 illustrates the AS-IS Eligibility and Enrollment data exchanges for OSDH.

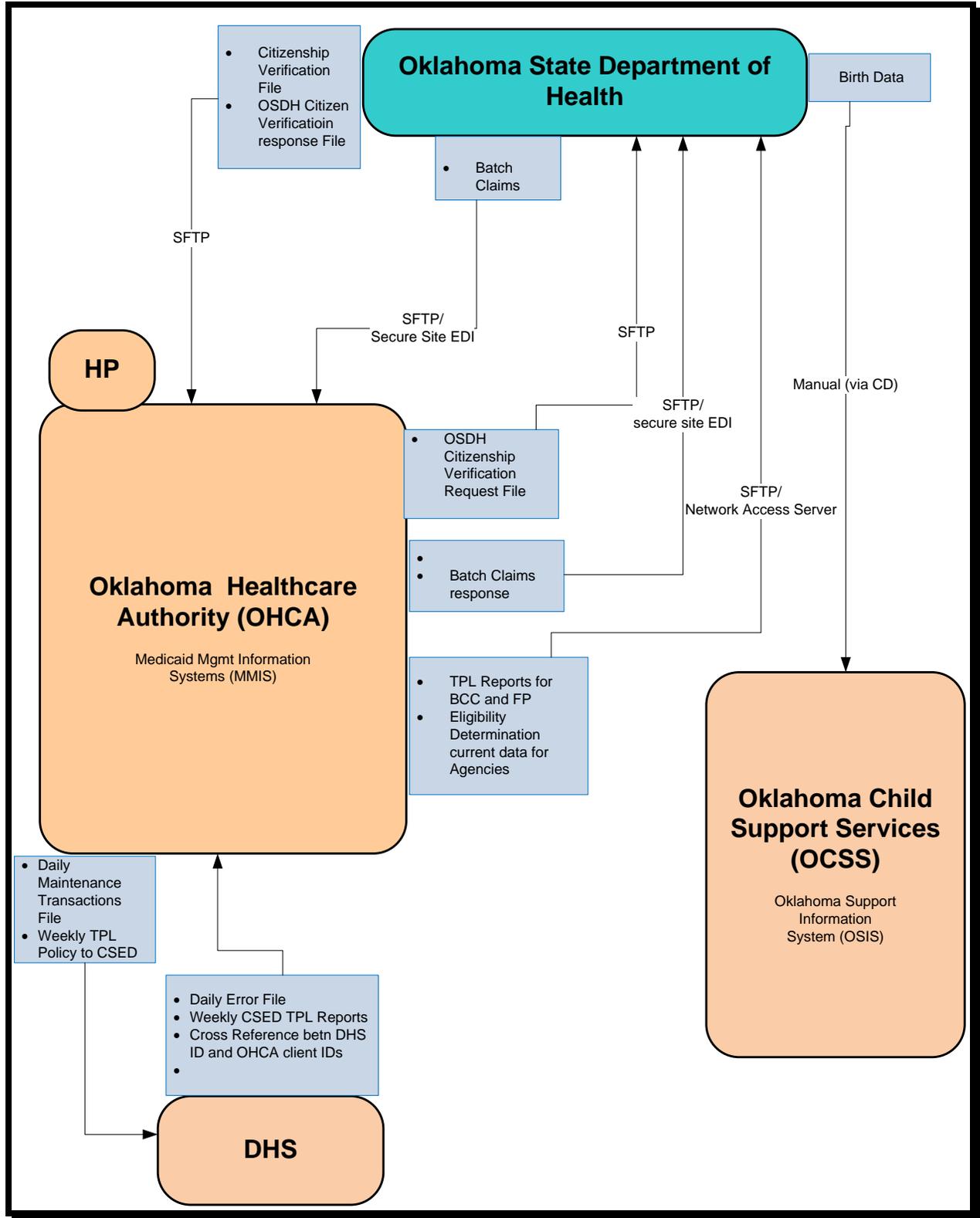


Figure A-15: Eligibility and Enrollment Interfaces for OSDH

7 STAKEHOLDERS

The following describes those integrated stakeholders and interface(s) between systems, agency(s) and internal/external customers that collaborate with the OMES, OHCA, OSDH and OKDHS which provides services for three Health and Human Services communities, CWS, OCSS and AFS.

7.1 Case Workers

OKDHS Case Workers – Directly access the data through user interfaces provided by the organizations that own the following systems:

- OSIS
- PS2
- KIDS
- MMIS

7.2 Clients

OCSS Clients (known as Customers to OCSS) access the following:

- OSIS via IVR
- Web Portal
- CARE Call Center

7.3 Federal Authorities

Federal Authorities – Directly access to OSIS via the user interface. OCSS participates in various interfaces provided by Federal authorities such as Federal Offset Program, Federal Identification Management (FIdM) multi State matching and Passport Denial for example.

7.4 Other States

Access OCSS data via interfaces provided by OCSE called State Services portal and CSENet.

7.5 Providers

- Collection Agencies
- Credit Bureaus
- District Attorney's Office
- Community Action Agency Office
- SMI (SDU vendor)
- Young-Williams

- Xerox
- Informatix (In state FIdM)
- Office of Administrative Court

7.6 Management

The same access as Case Workers to the various interfaces.

7.7 Reporting Module

OCSS, AFS, and CWS – Uses the same reporting module which are:

- WebFOCUS
- RDS/Document Direct

7.8 Oklahoma Public Health Module

- OCSS currently receives birth records and Acknowledgment of Paternity (AOP)
- OCSS needs adoption information but currently has no agreement.

7.9 Oklahoma Human Services Module

OCSS, AFS, and CWS – Uses the same reporting module which are:

- Department Client Numbering
- Adobe Live Cycle for document generation
- TANF, Foster Care, Medicaid, and Child Care Subsidy eligibility information
- Benefits expended for TANF, Foster Care, and Child Care Subsidy
- WebFOCUS
- RDS/Document Direct

7.10 Oklahoma Child Welfare Services (CWS) Module

CWS exchanges data (interfaces) with AFS, OHCA and OCSS. OCSS needs:

- Foster Care eligibility information
- Benefits expended for Foster Care
- Child Support orders that are established

7.11 Adult and Family Services (AFS) Module

AFS exchanges data (interfaces) with OCSS and OHCA.

7.12 Oklahoma Child Support Services (OCSS) Module

AFS, CWS, OHCA and OSDH exchanges data (interfaces) with OCSS.

7.13 Oklahoma Medicaid Services Module

OCSS – OHCA refers cases to OCSS that are required to participate in the Title IV-D program due to participation in the Medicaid program. OHCA and OCSS exchange Demographic information, child support order and payment information, TPL insurance information, Custodial Parents (CP) cooperation information, and eligibility information on participants in OHCA Medicaid cases. OCSS obtains orders and collects payments that are forwarded to OHCA to offset the cost of the Medicaid program.

OCSS has a very similar relationship with AFS and CWS. Case referrals are received and information is shared between the programs on case participants, child support orders and payment information, CP cooperation, and benefits expended. OCSS retains child support payments when an assignment of support rights is in effect and forwards retained collections to the Title IV-A and Title IV-E programs. OCSS also retains child support payments in Non-Title IV-E foster care cases and forwards these to CWS.

7.14 Oklahoma Providers Module

7.14.1 Oklahoma Health Care Authority (OCHA)

MMIS physical infrastructure includes high-bandwidth network components, industry-leading security, and full redundancy in support of the primary user groups: OHCA, external stakeholders, HPES operations, and the HPES account staff.

7.14.2 Oklahoma State Department of Health (OSDH)

OSDH Vital Records creates data sets for National Center for Health Statistics (NCHS) and SSA. It creates files from database and sends on media, through shared folders, FTP or other mechanisms.

APPENDIX A-1-1 – SUPPORTING DOCUMENTATION

To review the following referenced Appendices, A-1-1 through A-1-15, please refer to the accompanying file named: [Oklahoma 90FQ0006 Data Roadmap – Version 2.0_ Appendices.zip](#)

Contents of this file include the following:

- **OCSS Data Elements Appendix Directory:**
 - A-1-1.1 CSENet Dictionary.pdf
 - A-1-1.2 Carrier File.docx
 - A-1-1.3 AP File to OHCA.doc
 - A-1-1.4 OHCA Daily Referral File.docx
 - A-1-1.5 Agency User Manual.doc
 - A-1-1.6 CSENet Data Dictionary.pdf
 - A-1-1.7 Quick Data Elements.docx
 - A-1-1.8 G3 Messages.doc
 - A-1-1.9 APED CSED ABSENT PARENT EMPLOYMENT DETAIL UPDATE.docx
 - A-1-1.10 APUI CSED OESC UCB Data Inquiry.docx
 - A-1-1.11 AFS Data Screens.docx
 - A-1-1.12 Child Welfare Extract.docx
- A-1-1 AS-IS List of Eligibility and Enrollment Interfaces & Data Elements.xlsx
- A-1-2 AS-IS Data Elements Attachments for A-1-1.xlsx
- A-1-3 AS-IS Business Rules for Interfaces AFS CWS OCSS.xlsx
- A-1-4 NHSIA Conceptual Data Model.pdf
- A-1-5 NHSIAS IEPD NIEM Data Elements Mapping Template.xlsx
- A-1-6 NIEM Human Services Domain Governance Roles and Responsibilities.docx
- A-1-7 AS-IS Matching Criteria for all Agencies.xlsx
- A-1-8 List of NHSIA Information Exchanges.xlsx
- A-1-9 Mapping AS-IS Information Exchanges to NHSIA Information Exchanges.xlsx
- A-1-10 OSDH Agreement.pdf
- A-1-11 OHCA Agreement.pdf
- A-1-12 OHCA Change Order Process.doc
- A-1-13 OHCA Business Associate Agreement Template.doc
- A-1-14 OHCA Data Use Agreement.docx
- A-1-15 OCSS SPR.doc

APPENDIX B - PROGRAM MATRIX

Agency/Line of Business (LOB)	System Name	Program	Eligibility Intake	Intake (Face-to-Face, Interviews, Applications, etc.)	Determine Eligibility	Case Management (Enroll/ Dis-Enroll Client)	Inquiry, Monitoring (Reports)	Medical/ Medicaid
OKDHS - Oklahoma Child Support Services (OCSS)	Oklahoma Support Information System (OSIS)	Title IV-D of the Social Security Act		X	X	X	X	X
		Non-IV-D Pass-Through		X	X	X	X	
		State Case Registry		X	X	X	X	
		Voluntary Acknowledgements		X		X	X	
		State-wide Birth Records		X			X	
OKDHS – Adult and Family Services (AFS)	PS2	Adult Protective Services (APS)		X	X	X	X	
		Low Income Home Energy Assistance Program (LIHEAP)	X	X	X		X	
		Supplemental Nutrition Assistance Program (SNAP)	X	X	X	X	X	
		Temporary Assistance for Needy Families (TANF)	X	X	X	X	X	X
		Child Care	X	X	X	X	X	
		Title II						
		Title XVI						
		Medicaid (Title XIX) Eligibility	X	X	X	X	X	X
		Title V - SSI-DCP	X	X	X	X	X	X
		Electronic Payment Systems (EBT, ECC & EPC)						
		Aid to the Aged, Blind and Disabled - State Supplemental Payment	X	X	X	X	X	X

OKDHS - Child Welfare Service (CWS)	KIDS	Foster Care /Bridge	X	X	X	X	X	
		Investigation/Assessments	X	X	X	X	X	
		Permanency Planning				X	X	X
		Adoption			X	X	X	X
		Adoption Subsidy	X		X	X	X	X
		Guardianship Subsidy (? TANF)	X	X	X	X	X	X
Oklahoma Health Care Authority (OHCA)	Medicaid Management Information System (MMIS)	Medicaid (Title XIX)	X	X	X	X	X	X
		Health Insurance Exchange (HIE)* 1	X					
Oklahoma State Department of Health (OSDH)	PHOCIS (OSDH Client Information System)	Women, Infants and Children (WIC)	X	X	X	X	X	X
		Children First	X	X	X	X	X	X
		Child Guidance	X	X	X		X	X
		Family Planning (Title X)	X	X	X		X	X
		Early Intervention/SoonerStart	X	X	X	X	X	X
	OSIIS (Immunization Registry) & PHOCIS	Immunizations	X	X	X		X	X
	Vital Records	Citizenship Verification/Medicaid Contract w/OHCA						X
	PHOCIS & BCC Grant Reporting System	Take Charge/Breast & Cervical Cancer Screening Program	X	X	X	X	X	X
	OHCA - MMIS	OK Cares/Breast & Cervical Cancer Rx Act	X	X				X
OHCA - Online Enrollment	Agency Partner - OSDH w/OHCA	X	X				X	

OKDHS - Aging Services Division (ASD)		Nursing Home (Intermediate Care Facility) Care and ADvantage Waiver (Medicaid funded home and community-based waiver)	X	X	X	X	X	X
OKDHS - Developmental Disabilities Service Division		Community Waiver, Family Support Assistance Payment, Homeward Bound Waiver, In-Home Supports Waiver for Adults, In Home Supports Waiver for Children, Intermediate Care Facilities for the Mentally Retarded	X	X	X	X	X	X
<p>* Oklahoma will not have an exchange of its own. OHCA will coordinate with the fed exchange but not have any control over it. 1 OHCA will intake info and if the applicant is not eligibility for Medicaid we will send info to the exchange. details unknown at this time.</p>								