
90FQ0006
Oklahoma Interoperability Grant
**Service-Oriented Architecture
(SOA) 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 Signature

Signature on File in Project Files

Karen Philbin, 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	Karen Philbin	Edits, additions and sequencing
02.20.2013	Rev. – 1.0	Karen Philbin	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	6
1.1	Purpose	6
1.1.1	Goals/Objectives.....	6
1.1.2	Project Outcomes	7
1.2	Assumptions and Constraints.....	8
1.3	Benefit to Other States	9
1.4	Breadth.....	9
1.5	Human Services Program and Initiatives.....	9
1.6	Information Technology Initiatives	10
1.7	Health Intersection.....	11
1.8	End Result.....	11
1.9	Background/Overview	11
1.9.1	Service-Oriented Architecture and Service-Oriented Systems	12
1.9.2	Services	12
1.9.3	Exploration Questions/Answers	12
1.9.4	Options Considered	14
1.9.5	Options Impact and Goals	14
1.9.5.1	Improve service delivery for clients	14
1.9.5.2	Reduce Errors and Improve Program Integrity.....	15
1.9.5.3	Improve Administrative Efficiency	15
2	Architecture Frameworks	15
2.1	Building a(n) SOA Roadmap	16
2.2	National Human Services Interoperability Architecture (NHSIA)	18
2.3	Architecture Viewpoints.....	19
2.4	Implementing NHSIA.....	24
3	AS-IS OVERVIEW.....	25
4	Governance.....	28
4.1	AS-IS Governance.....	29
4.1.1	OKDHS – IT Governance Model.....	29
4.1.2	OHCA – IT Governance Model	29
4.1.3	OSDH – IT Governance Model	30
4.1.4	Overall Current Governance Structure.....	30
4.1.5	State of Oklahoma – Enterprise IT Governance Model	31
5	TO-BE SOA Strategy	33
5.1	TO-BE System Overview.....	33
5.1.1	Step 1: Define the SOA Reference Architecture	34
5.1.2	Step 2: Define the SOA Roadmap	39
5.1.3	Step 3: Define the Governance Strategy	40
5.2	TO-BE Security Requirements	43

5.2.1	Policies and Procedures	45
5.2.2	Web Services Security.....	45
5.2.3	Security for Web Services and Windows Communication Foundation (WCF) Services.....	46
5.2.4	Security for Databases.....	46
5.2.5	Exceptions	47
5.3	TO-BE SOA Interfaces	47
5.3.1	SOA and the Enterprise Service Bus (ESB)	47
5.3.2	Message Oriented Middleware (MOM)	48
5.4	TO-BE Web Services	48
6	Recommended Approach	49
6.1	The SOA Roadmap	49
6.1.1	Construct and Maintain Master Services Portfolio	49
6.1.2	Implement Cross Enterprise Security	49
6.1.3	Extend the Scope of SOA Solutions to Span Multiple Business Units	50
6.1.4	Extend the Scope of SOA Solutions to External Business Partners	50
6.1.5	SOA Communication and Update of Applicable Knowledge Portal	50
6.1.6	Develop Target Enterprise SOA Architecture	51
6.1.7	Specify SOA Policies and Procedures.....	51
6.1.8	Integrate SOA Principles into Organization Wide SDLC	51
6.1.9	Develop and Implement SOA Lifecycle Governance	52
6.1.10	Summary of SOA Governance Strategy outlined earlier:.....	52
6.1.11	Ensure Ongoing Partnership between IT and Business	52
6.1.12	Ensure Executive Commitment and Sponsorship for SOA Program	53
6.1.13	Provide SOA Training and Certification	53
6.1.14	Monitor and Report on Service Performance.....	53
6.1.15	Implement Services Using ESB.....	53
6.1.16	Potential Sequence of SOA Initiatives	53
6.2	Summary	54
7	Acronyms.....	55
	APPENDIX A – AS-IS SYSTEM INTERFACES	A-1
	APPENDIX B – AS-IS AGENCY PROGRAMS	B-1
	APPENDIX C – AS-IS SYSTEMS OVERVIEW	C-1

List of Tables

Table 1: Goals/Objectives	7
Table 2: Project Outcomes.....	7
Table 3: Exploration Questions/Answers.....	12
Table 4: NHSIA and MITA Comparison.....	21
Table 5: Web Services Security	45

List of Figures

Figure 1: Identify AS-IS and TO-BE	16
Figure 2: NHSIA Core Supports All Business Areas	17
Figure 3: Architecture Levels and Attributes.....	19
Figure 4: NHSIA Architecture Viewpoints.....	20
Figure 5: NHSIA Architecture Viewpoint Descriptions.....	21
Figure 6: NHSIA Provides a Framework for Shared Business Processes.....	22
Figure 7: Shared IT Infrastructure	23
Figure 8: Notional NHSIA Roadmap.....	23
Figure 9: Steps to Implement NHSIA	25
Figure 10: AS-IS System Overview.....	26
Figure 11: AS-IS System Overview/Data Exchanges.....	Error! Bookmark not defined.
Figure 12: Current Governance Structure	31
Figure 13: Governance Structure	32
Figure 14: IT Governance Organizational Structure.....	32
Figure 15: IT Governance Organizational Structure.....	33
Figure 16: TO-BE Enterprise Architecture.....	34
Figure 17: SOA Reference Architecture	35
Figure 18: NHSIA Systems Reference Model Layers.....	36
Figure 19: SOA Governance IT and Enterprise Architecture Governance	41
Figure 20: SOA Governance with the Enterprise	41
Figure 21: Identity Management & Access Control	44
Figure 22: Potential SOA Initiative Sequence	54

1 EXECUTIVE SUMMARY

1.1 Purpose

Oklahoma is exploring and planning for improved interoperability and integration in eligibility and enrollment, case management, and other related functions across human services IT systems as well as exploring integration with other programs.

This interoperability exploration and planning effort includes developing a roadmap for integration of Service Oriented Architecture (SOA) and Enterprise Service Bus (ESB) to allow interoperability, fully automated data exchange and service reusability for all services exchanged between Oklahoma Department of Human Services (OKDHS), Oklahoma Health Care Authority (OHCA), Oklahoma State Department of Health (OSDH) and other initiatives. In addition to the inter-agency interoperability initiatives, intra-agency initiatives for interoperability exist between three main business unit divisions within OKDHS. These include Oklahoma Child Support Services (OCSS), Adult and Family Services (AFS) and Child Welfare Services (CWS).

Currently OSDH is working independently on one interoperability plan, while OHCA is working on another interoperability plan and now OKDHS, partnering with the Office of Management and Enterprise Services (OMES), is developing a third interoperability plan. These separate efforts are creating disjointed plans and possible inefficiencies. The intent is to come up with a unified overall interoperability plan that can improve data exchange processes, increase data quality and reusability, reduce errors and enhance data integrity between all the agencies.

The purpose of this SOA Roadmap is to provide OKDHS and its collaborating agencies with guidance regarding typical activities and initiatives that need to be executed as part of the SOA journey.

This SOA roadmap will continually be updated as decisions are made and details are further defined.

This project will provide opportunities for inter-agency collaboration and allow multiple State agencies to leverage 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

Goal/Objective	Desired Outcome	Measurement	Impact
Standardization	<i>Enterprise wide standards</i>	<i>Adopted by Inter/Intra Agencies and Programs</i>	<i>Improved efficiency</i>
Reusability	<i>Shared & reused data</i>	<i>Adopted as a model by other states</i>	<i>Reduction of development time</i>
Reduce Data Redundancy	<i>Less data redundancy & improved data consistency</i>	<i>Adopted by Inter/Intra Agencies and Programs</i>	<i>Improved data integrity and reduced errors</i>
Governance	<i>Policies and procedures</i>	<i>Adopted by Inter/Intra Agencies and Programs</i>	<i>Conformance to standards</i>
Cost	<i>Reduced operating expenses</i>	<i>Less operating and maintenance costs</i>	<i>Consolidated maintenance and shared operating costs</i>
Shared Services	<i>Interoperability</i>	<i>Adopted by Inter/Intra Agencies and Programs</i>	<i>Improved agility, response times, interoperability</i>
NHSIA adoption	<i>Interoperability</i>	<i>Adopted by Inter/Intra Agencies and Programs</i>	<i>Improved agility, response times, interoperability</i>
NIEM adoption	<i>Interoperability and use of standards</i>	<i>Adopted by Inter/Intra Agencies and Programs</i>	<i>Improved agility, response times, interoperability</i>
MITA compliance	<i>Interoperability and use of standards</i>	<i>Adopted by Inter/Intra Agencies and Programs</i>	<i>Improved agility, response times, interoperability</i>

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: Project Outcomes

Index	Project Outcomes
O1	This project provides opportunities for intra-agency and inter-agency collaboration. It allows OKDHS and multiple State agencies to leverage SOA services and capabilities, in support of the state’s effort to meet the timelines of the ACA for citizen enrollment. Leveraging SOA will provide for reusability and better data exchange to improve outcomes for vulnerable children and improve service delivery for clients.
O2	The interoperability plan and SOA roadmap will outline compliance with the Seven Conditions and Standards as outlined by Centers for Medicare and Medicaid Services (CMS) and CMS Guidance for Exchange and Medicaid Information Technology (IT) Systems Version 2.0. The Seven Conditions and Standards include: <ol style="list-style-type: none"> 1. Modular Systems Development 2. Align with MITA 3. Industry Standards

	<ol style="list-style-type: none"> 4. Share and Re-Use Technology (Leverage Condition) 5. Deliver Business Results 6. Performance Reporting 7. Interoperability <p>The plan and roadmap will incorporate Medicaid Information Technology Architecture (MITA) Maturity Model (MITA Framework Version 3.0) principles, National Human Services Interoperability Architecture (NHSIA) which provides a context for standardized data sharing by incorporating the use of National Information Exchange Model (NIEM), and SOA Integration Framework.</p>
O3	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 of web services to support these processes can transform administrative activities to reduce redundancy of effort and streamline workflows to improve efficiency.
O4	Develop a roadmap for integration of SOA/ESB to allow fully automated data exchange and service reusability for all services exchanged between OKDHS and OHCA and other initiatives.

1.2 Assumptions and Constraints

Assumptions and constraints that influenced preparation of this document include:

- **Schedule Constraints:** Delayed start on Interoperability Planning Grant, scheduled contingent upon approval of SOA Roadmap.
- **Data Constraints:** To narrow and manage the project scope, the initial focus is on Eligibility and Enterprise Master Person Index (eMPI), and data exchanges between agencies and/or programs.
- **Hardware Constraints:** Any required hardware must fit with SOA and Enterprise Architecture and acquisition of any additional hardware is dependent on funding or financial constraints.
- **Software Constraints:** Any required developed or Commercial off The Shelf (COTS) software must fit within the approved SOA and Enterprise Architecture, and acquisition of any additional software is dependent on funding or financial constraint.
- **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.
- **Security Constraints:** Security mandates must be followed regarding the handling of Internal Revenue Service (IRS), Health Insurance Portability and Accountability Act (HIPAA), Social Security Administration (SSA) and any federal tax information.
- **Political Constraints:** Local, state or federal laws or 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 (MOA) 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.

1.3 Benefit to Other States

This Interoperability Plan may be used by other states to implement Enterprise Interoperability measures.

1.4 Breadth

The focus of this interoperability effort will include: state and federal programs that require eligibility determination: Supplemental Nutrition Assistance Program (SNAP), Temporary Assistance to 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 CWS, OCSS, 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 OSDH’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.

1.5 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.

1.6 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 ACA 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). The proposed system will also 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
- Children’s Health Insurance Program (CHIP)
- Basic Health Program, if established by the state

MITA ensures the availability of high-quality health care coverage to families and individuals are achieved through a collaborative partnership between and within federal agencies and states responsible for implementation of the Exchanges and the ACA’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.

1.7 Health Intersection

Currently Oklahoma has elected to not participate in the Federal Health Insurance Exchange (HIE), nor have an Exchange. However, the OHCA will coordinate with the Federal Exchange in a yet to be determined process by conducting their own intake process and determining eligibility.

Additional Interoperability between NHSIA and MITA Programs for Oklahoma can be reviewed with Appendix A. Plans are to support a future exchange interoperability concept.

OSDH is seeking a comprehensive solution for an Interoperable Public Health Information System (IPHIS), to prepare for participating with health information exchange activities and to improve the quality of data available to support decisions about improving the health of Oklahomans.

1.8 End Result

Interoperability is the expected end result. Implementation of SOA/ESB under a NHSIA/MITA/NIEM framework guidance is the expected vehicle to achieve interoperability. An eMPI is also an expected end result.

1.9 Background/Overview

SOA has emerged as a crucial enabling technology for interoperability among disparate pieces of software regardless of the network architecture, platform, or programming language. SOA is a conceptual framework for designing and building networks and Web services that allow for data to be exchanged where and when it is needed. SOA is a client/server design approach in which an application consists of software services and software service consumers (also known as clients or service requesters).

SOA differs from the more general client/server model in its definitive emphasis on loose coupling between software components, and in its use of separately standing interfaces (Gartner). SOA raises the bar in terms of quality in service offerings. Services

are used by clients/partners, and implicit in their use is a trust – a trust that the service will be stable and always work as expected.

*SOA is an architectural approach to building systems which involves applications being exposed as “services”. This approach delivers two major values, sharing and agility. Sharing provides leverage and reuse. Agility provides the capability to change more rapidly. SOA is accomplished through two fundamental principles: interface abstraction and modularization. There are five criteria for an SOA application: modular, distributed, discoverable, swappable, and shareable.
From SEI – Carnegie Mellon*

1.9.1 Service-Oriented Architecture and Service-Oriented Systems

SOA is a way of designing, developing, deploying, and managing systems, in which services provide reusable business functionality via well-defined interfaces. There is a clear separation between service interface and service implementation. Service consumers are built using functionality from available services. An SOA infrastructure enables discovery, composition, and invocation of services. Protocols are predominantly, but not exclusively, message-based document exchanges.

From a more technical point of view, SOA is an architectural style or design paradigm; it is neither system architecture nor a complete system. Systems that are built based on the SOA characteristics listed above are called service-oriented systems.

1.9.2 Services

Services are reusable components that represent business or operational tasks, such as customer lookup, credit card validation, weather lookup, or line-of-sight calculation. Reusable is a key element of this definition because it is what enables the creation of new business and operational processes based on these services. Services expose their capabilities via well-defined, standard service interfaces. In a service-oriented environment, service interface definitions are available in some form of service registry.

If systems are built as components, then each system can be developed and maintained independently. SOA is a set of design patterns that guide the building and integration of these mini-application pieces.

1.9.3 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	Questions/Answers
Q1	What resources will be needed to integrate OKDHS human services programs into MITA Maturity Model (MITA Framework Version 3.0)/ NHSIA compliant architecture?

A1	Business and technical resources will be needed to adopt and implement MITA and NHSIA. It will depend on the level of adoption. Resources may include architects, business process engineers, developers, and most importantly executive leadership to provide organizational commitment.
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	SOA and ESB architectures will be needed. Identity management and access control is needed including strong authentication. Network and infrastructure security also make up the security architecture. The Global Federated Identity and Privilege Management (GFIPM) could be used for federated identity and privilege management to allow users from one federation partner to seamlessly access resources from another partner in a secure and trustworthy manner.
Q3	What is needed among the health and human services agencies to develop and share eMPI?
A3	<p>This is under review although it is known that coordination and collaboration is needed. Research is underway to determine the extent of current level of effort already done by OHCA and OSDH in planning to share eMPI services. Expectations are that sharing software, licensing and expertise will provide longer term cost benefits.</p> <p>The participating agencies were questioned as to the matching criteria that they use in their systems to identify a person. Except OSDH, all other agencies thought the idea of applying Master Data Management (MDM) technology would be a valuable approach when focusing on eMPI for interoperability. Leveraging the eMPI concept by utilizing MDM and storing in a master data for ease of access and sharing would reduce errors, maintenance and cost of the stored data. OSDH has a state mandate that Birth information is only released to certain designated agencies and their data cannot be shared for eMPI purposes.</p>
Q4	What initiatives of the MOSAIC human services eligibility and case management system can be shared with OHCA initiatives under the ACA?
A4	MOSAIC initially focused on the three largest business divisions of OKDHS. MOSAIC is currently being considered at an enterprise level. Initiatives of the proposed MOSAIC system will be reviewed to determine which can be shared with OHCA for ACA efforts.
Q5	What efficiencies can be gained by using SOA?
A5	Sharing and agility are the major values of SOA which provide efficiencies. Sharing provides leverage and reuse. Agility provides the capability to change more rapidly. SOA helps with silos by creating interoperability agreements that reconcile how systems talk to each other, the data formats they use, and the organizational barriers to cooperation.
Q6	How can governance be used to achieve the wide range of performance expectations?
A6	Governance is critical. SOA governance is a combination of best practices to help combat sprawl. Through governance, service-level agreements can be established to define performance expectations as well as measurements that confirm that services are performing as expected.
Q7	How can Oklahoma improve overall State IT operating and cost efficiencies?
A7	Increasing interoperability and developing reusable, standardized services will drive

costs down and improve efficiencies. Adoption of NHSIA, MITA, NIEM, SOA and ESB implementations will assist in this effort.

1.9.4 Options Considered

As part of the SOA Roadmap development, several different Enterprise Architecture (EA) frameworks and methodologies were reviewed. The Zachman Framework, The Open Group Architecture Framework (TOGAF), Federal Enterprise Architecture (FEA) and Department of Defense (DoD) Architectural Framework (DoDAF) were reviewed. SOA Methodologies and SOA Maturity Models were also reviewed to determine potential usefulness and appropriateness for adoption by Oklahoma. SOA maturity models from Microsoft, IBM, Oracle and The Open Group Service Integration Maturity Model (OSIMM) Version 2 have been reviewed. These maturity models provide a framework and a roadmap much like MITA does.

The NHSIA developed by the Administration for Children and Families (ACF) is a framework to support integrated eligibility determination and information sharing across programs and agencies. NHSIA focuses on enabling information exchange and sharing IT services among information systems.

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.

1.9.5 Options Impact and Goals

1.9.5.1 Improve service delivery for clients

The implementation of SOA across state agencies will benefit 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.

1.9.5.2 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 a statewide eMPI:

- Errors can be reduced
- Accuracy of eligibility determinations increased.

Information reported to or available in one program can be shared with other programs in support of program integrity efforts.

1.9.5.3 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 ARCHITECTURE FRAMEWORKS

The scope of this interoperability exploration and planning effort includes developing a roadmap for integration of SOA and ESB to allow interoperability, fully automated data exchange and service reusability for all services exchanged between OKDHS, OHCA, OSDH and other initiatives. In addition to the inter-agency interoperability initiatives, intra-agency initiatives for interoperability exist between three main business unit divisions within OKDHS. These include OCSS, AFS and CWS.

OKDHS hopes to embrace SOA as a business-IT strategy. The development of a roadmap for implementing SOA to provide better alignment between business and IT is an effort to improve interoperability. As previously stated, several architecture

frameworks have been reviewed. This section will highlight the frameworks targeted for use by Oklahoma and their importance.

2.1 Building a(n) SOA Roadmap

Typically, all roadmap building follows the same four steps:

- Where are we now? (current state or AS-IS)
- Where do we want to be? (desired future state or TO-BE)
- What is the gap between the two? (gap analysis)
- What is the path to get to where we want to be? (roadmap to TO-BE)

The approach used in this roadmap is to identify the current state or AS-IS architecture and identify the future SOA state or TO-BE architecture and analyze the gaps between the two. This will provide a clear understanding of where we are and where we want to be.

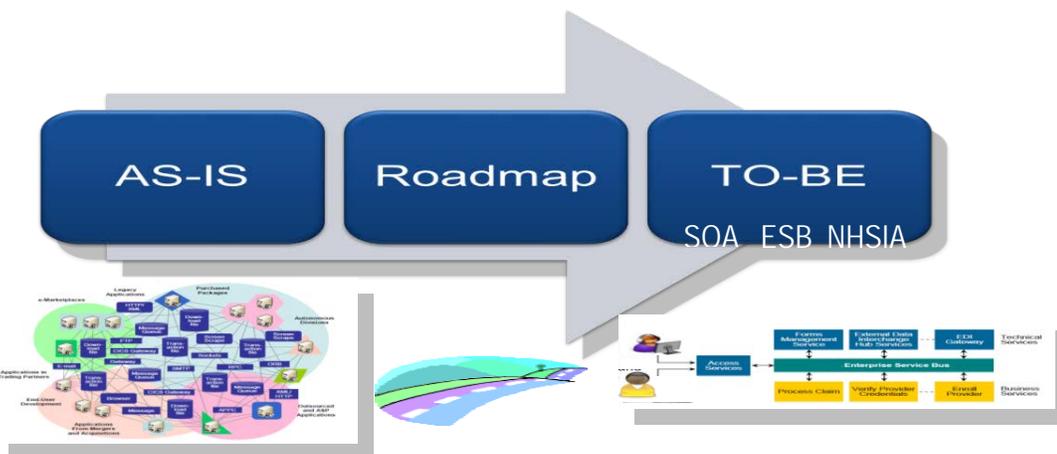


Figure 1: Identify AS-IS and TO-BE

The approach that NHSIA takes is to architect a core set of essential capabilities that everyone needs. The core capabilities enable critical information sharing and create an environment that allows new capabilities to evolve more easily. The core NHSIA capabilities:

- Provide a foundation for interoperability
- Provide foundational capabilities or information

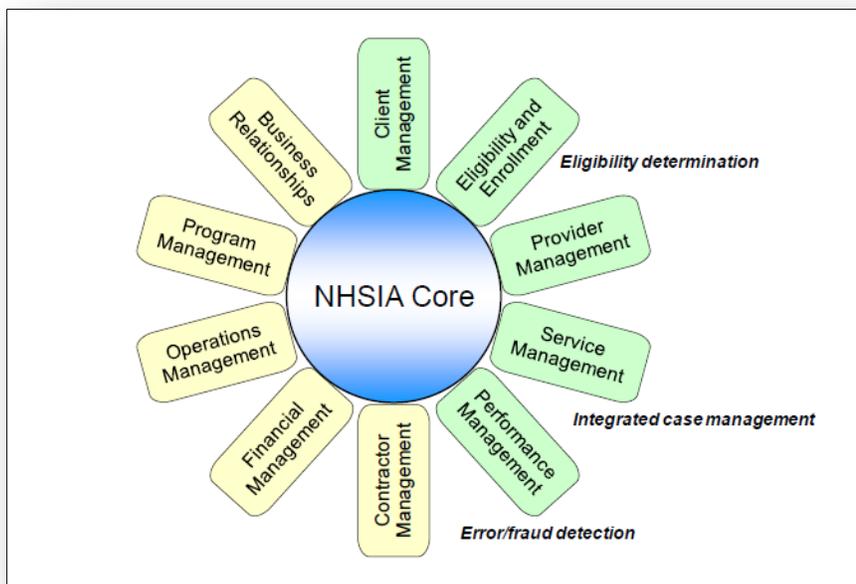


Figure 2: NHSIA Core Supports All Business Areas

Figure 2 illustrates that the NHSIA core supports all the business areas involved in human services. Initial work on NHSIA addressed the business areas covering client management, eligibility and enrollment, provider management, service management, and performance management in some detail. Other business areas including business relationships, program management, operations management, financial management and contractor management defined at a high level. The core elements provide functionality upon which end-user capabilities can be built.

Implementing NHSIA core concepts means that these core information system elements will be available:

- A SOA infrastructure which provides the foundation for IT service discovery and re-use.
- A set of hubs to share IT services. Information sharing should use NIEM-based standards. The initial shared IT services and information sets are those required to support core capabilities.
- For authorized users, single sign-on and attribute-based access control to streamline the user's experience and abide by confidentiality agreements.
- A set of repositories to facilitate selected data aggregation and analysis.

In order to define the NHSIA framework we have to review and attain a clear understanding of NHSIA. Many aspects of the approach outlined in NHSIA are based on methodologies recommended in the Global Reference Architecture (GRA) that has been published by the Department of Justice. NHSIA extends the MITA model to encompass the Human Service Domain.

MITA is an evolving CMS initiative that fosters an integrated business, information and technological approach to building management systems that are client-based and capable of sharing information across organizational silos based upon nationally recognized standards.

NHSIA takes the MITA concepts and principles and extends them beyond Medicaid to apply to human services. Therefore, an understanding of GRA and MITA would be helpful.

The approach taken in developing this roadmap will include the following steps:

- Review NHSIA
- Define NHSIA Framework as it applies to Oklahoma
- Analyze AS-IS Environment
- Define NHSIA Capabilities
- Define SOA Reference Architecture
- Define TO-BE Architecture

A thorough review of NHSIA is underway. Additional NHSIA information will be detailed in section 5.1 TO-BE System.

Systems involved in the Interoperability project are OSDH, OHCA, CWS, OCSS, and AFS. These systems have various types of data that are being exchanged via interfaces. Interfaces could be Real-Time (data is accessed directly any day/anytime), Transactional or Transfer (push/pull via ftp services).

2.2 National Human Services Interoperability Architecture (NHSIA)

NHSIA proposes an architecture framework to facilitate information sharing, improve service delivery, prevent fraud, and provide better outcomes for children and families. NHSIA is enterprise architecture, the enterprise being the provisioning of human services across the nation. This national enterprise is large, and comprises many lower level enterprises. Therefore, NHSIA can be thought of as a multi-enterprise or community architecture.

NHSIA is part of a rough hierarchical set of related architectures as illustrated in Figure 3. The scope, level of detail, and content of these architectures often do not dovetail in a simple, structured way. Nevertheless, NHSIA should be developed with an understanding of these related architectures to ensure interoperability and avoid duplication. The architectures are federated; each level has a scope and purpose and is defined to an appropriate level-of-detail as summarized in Figure 3.

Level	Scope	Detail	Impact	Audience
Community Architecture	Multiple Organizations	Very Low	Community Outcomes	Community Stakeholders
Enterprise Architecture	Agency/ Organization	Low	Strategic Outcomes	Enterprise Stakeholders
Segment Architecture	Line of Business	Medium	Business Outcomes	Business Owners
Solution Architecture	Function/ Process	High	Operational Outcomes	Users & Developers

Figure 3: Architecture Levels and Attributes

2.3 Architecture Viewpoints

A best practice in architecting is to describe architecture in terms of multiple viewpoints. Each viewpoint serves the needs of a specific user or group, such as an executive manager making investment decisions, an operational user of the systems, or a systems developer designing data structures, services, and applications.

The DoDAF has evolved over a decade to include multiple viewpoints. NHSIA has adapted DoDAF to include the viewpoints shown in Figure 4. The adaptations include merging the DoDAF Systems and Services Viewpoints into a single Systems Viewpoint and pulling out an Infrastructure Viewpoint as a separate item from the Systems Viewpoint.

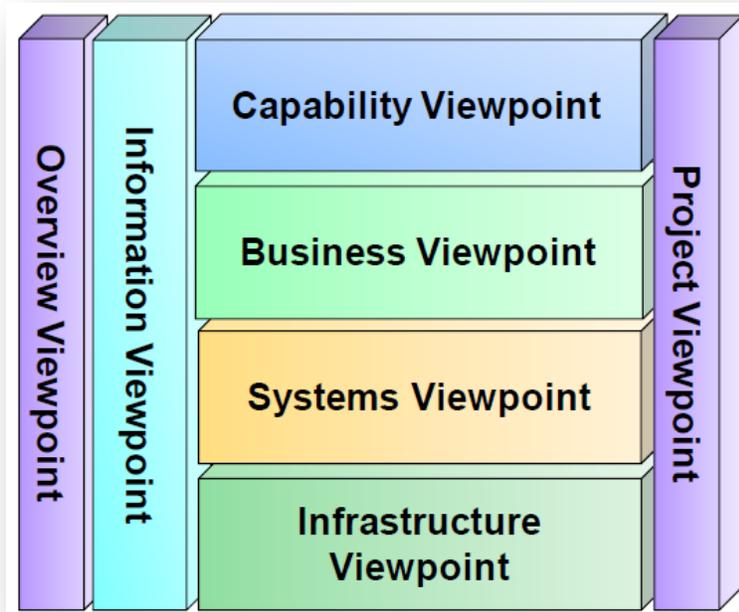


Figure 4: NHSIA Architecture Viewpoints

Figure 5 below defines the NHSIA Architecture Viewpoints.

Overview	Overarching aspects of architecture context that relate to all views, e.g. key concepts
Information	A conceptual data model (including high-level data classes, associations, attributes) and standards for data exchanges
Capability	Required high-level operational capabilities described in terms easily understood by decision makers and used to communicate a strategic vision. Includes a NHSIA scorecard and performance reference model.
Business	Business processes and operational scenarios
Systems	Describes new and legacy system components in the layers of the to-be architecture including software applications and services: their context, components, functions, and interfaces.
Infrastructure	The IT environment including networks, computing facilities, servers, and enterprise services
Project	Strategies and projects planned or required to implement the capabilities defined by the architecture

Figure 5: NHSIA Architecture Viewpoint Descriptions

Since there is some familiarity with MITA, it is helpful to compare MITA with NHSIA. MITA provides a common framework in the Medicaid arena to focus on opportunities to build common and shared services by decoupling legacy systems and processes and breaking down silos. Table 4 shows how NHSIA and MITA are closely aligned.

Table 4: NHSIA and MITA Comparison

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

NHSIA makes extensive use of the MITA Business Architecture and uses it as the basis for the NHSIA Business Viewpoint.

NHSIA provides a framework for shared business processes and understanding processes common across programs. This will help identify capabilities and processes that can be shared or reused across programs.

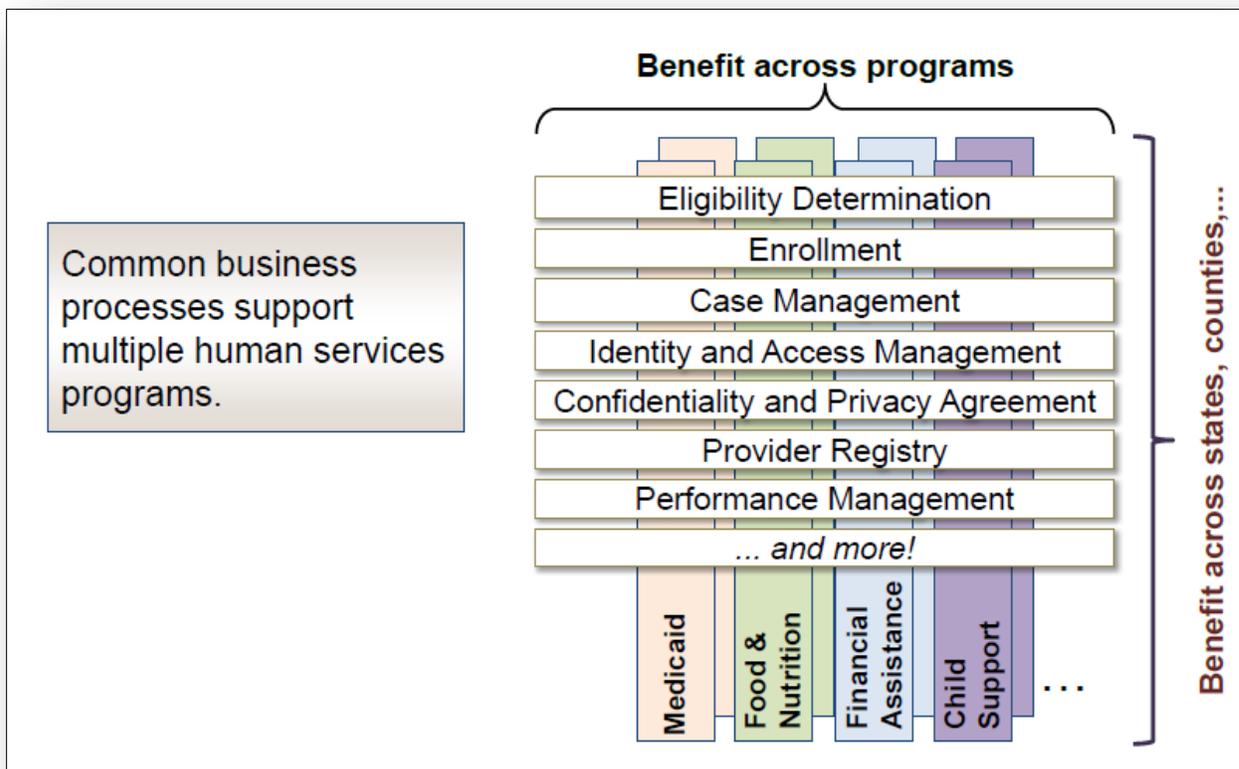


Figure 6: NHSIA Provides a Framework for Shared Business Processes

NHSIA addresses the interoperability problem by breaking down the barriers of siloed systems and promotes sharing information and applications across multiple human services programs. It is also possible to share the underlying infrastructure across human services programs. Technologies such as SOA make it possible to share the underlying hardware, network and systems software across multiple human services programs as depicted in Figure 7.

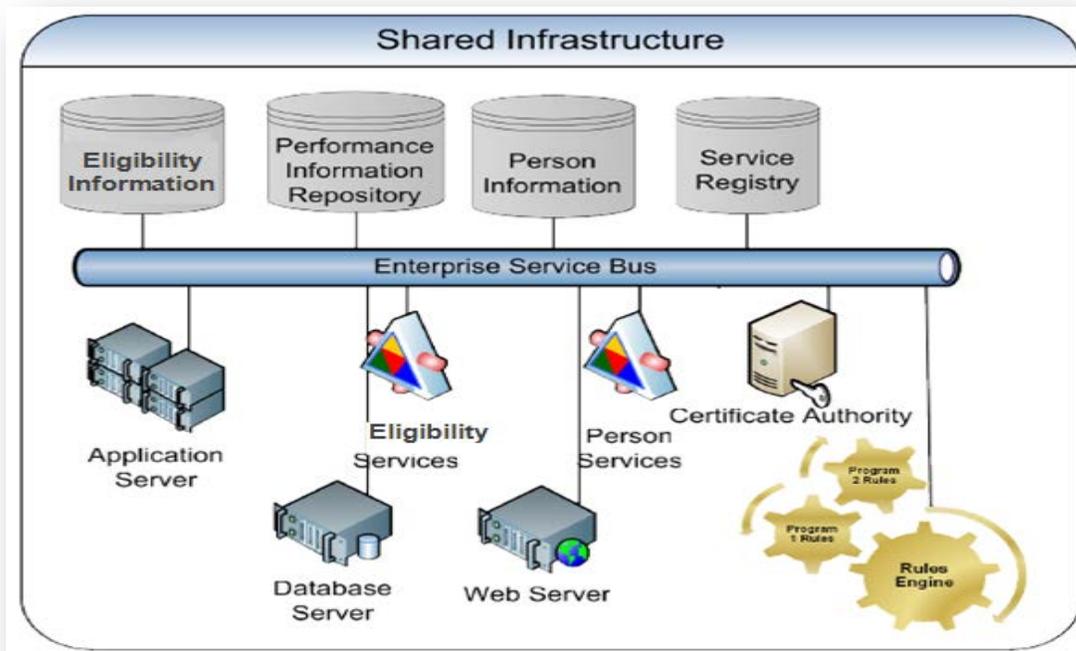


Figure 7: Shared IT Infrastructure

Implementing the complete, long term TO-BE environment envisioned by NHSIA would be a large effort, and probably not attainable in the near term given the level of available resources. In order to scope to a manageable effort, Oklahoma’s NHSIA team may initially focus on clearly defining and implementing the NHSIA core capabilities. A multi-year effort is envisioned as illustrated in Figure 8.

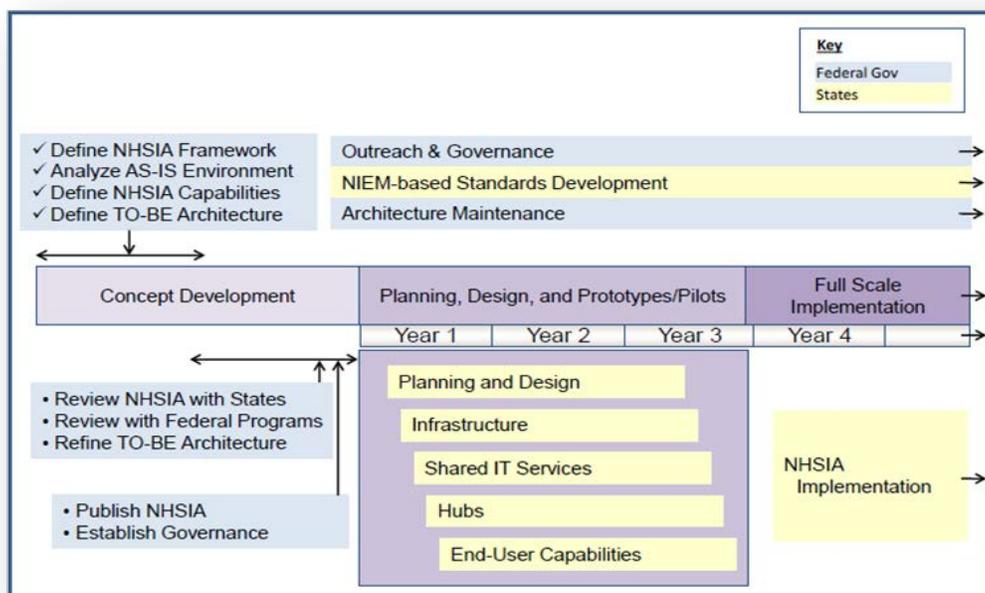


Figure 8: Notional NHSIA Roadmap

In Figure 8, federal government activities and state government activities are shown. Completed federal activities include defining the NHSIA framework, analyzing the AS-IS environment, defining NHSIA capabilities, and defining a draft to-be architecture. Future activities include reviewing NHSIA with states, reviewing with federal programs, refining and publishing NHSIA, and establishing governance. Outreach, governance, and architecture maintenance will be longer-term federal activities.

The roadmap shows state governments starting with planning, design, and prototypes/pilots, and then shifting to full-scale NHSIA implementation. The initial planning, design, and prototypes/pilots might include establishing core infrastructure, shared IT services, hubs, and initial end-user capabilities. Development of NIEM-based standards for information exchange is likely to be a longer-term activity.

The funding and acquisition of the NHSIA components may take many forms. There is no single acquisition approach for all of NHSIA implementation.

2.4 Implementing NHSIA

The steps recommended for the State to follow for implementing NHSIA:

- Assess Current Situation
- Plan and Design
- Support NIEM Standards Development
- Conduct NHSIA Prototypes and Pilots
- Update Plan and Design
- Implement NHSIA Incrementally

See Figure 9 for steps recommended by NHSIA.

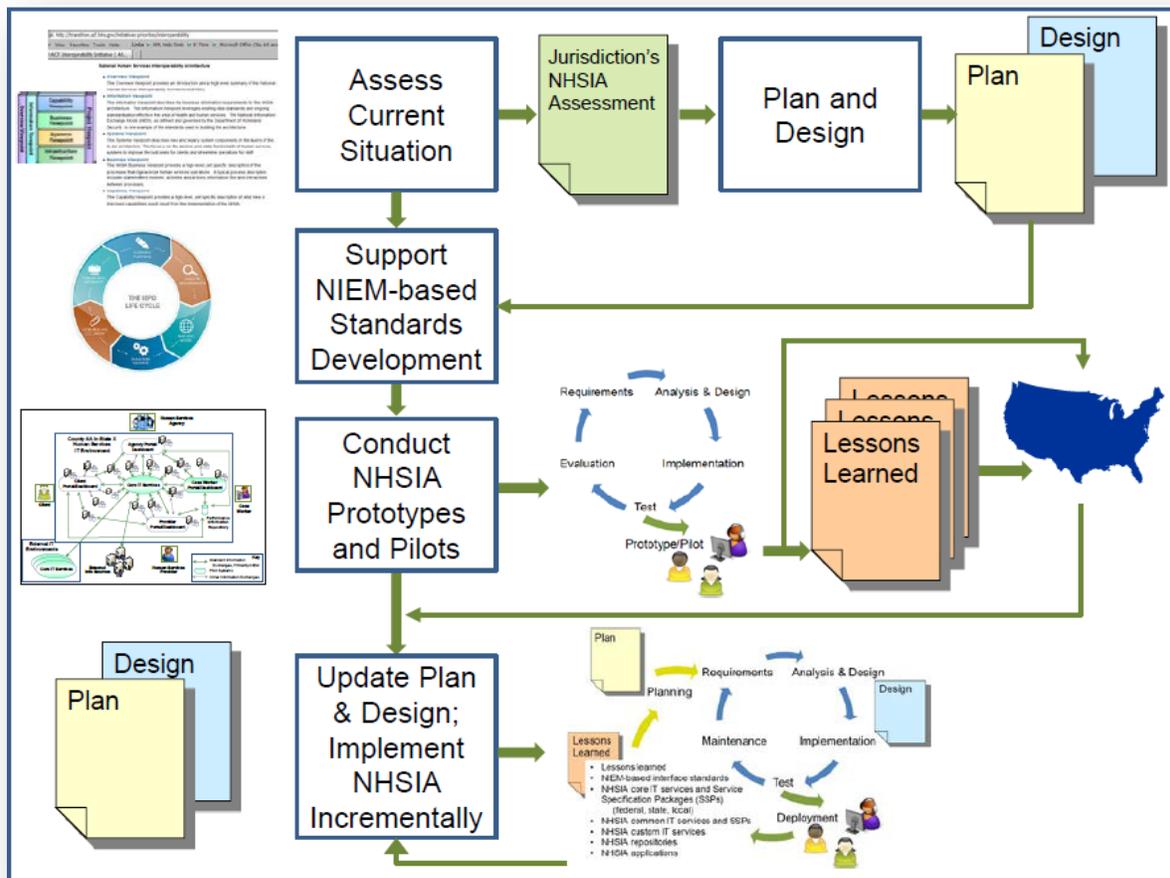


Figure 9: Steps to Implement NHSIA

3 AS-IS OVERVIEW

Figure 10 below shows the entities involved which include: OKDHS agencies (e.g., PS2 - AFS, Oklahoma Support Information System (OSIS) - OCSS, KIDS –CWS), and other departments and organizations (e.g., OHCA - Medicaid Management Information System (MMIS), OMES, OSDH).

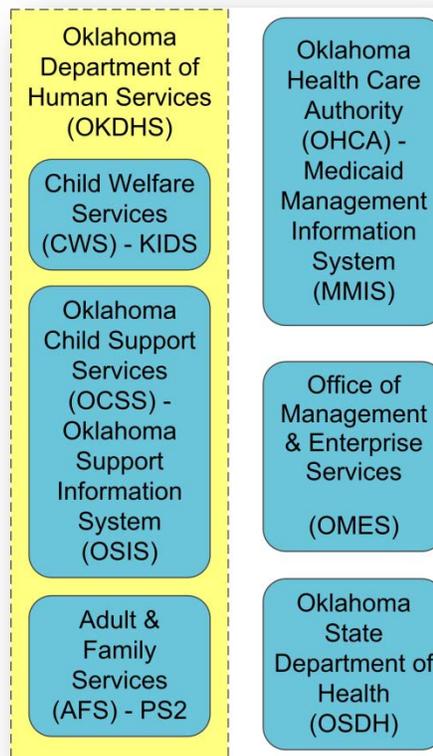


Figure 10: AS-IS System Overview

Figure 11 below illustrates the AS-IS data exchanges among agencies with a focus on Eligibility and Enrollment.

90FQ0006 Oklahoma Interoperability Grant Project
 Service-Oriented Architecture (SOA) Roadmap, Revision 2.0 April 26, 2013

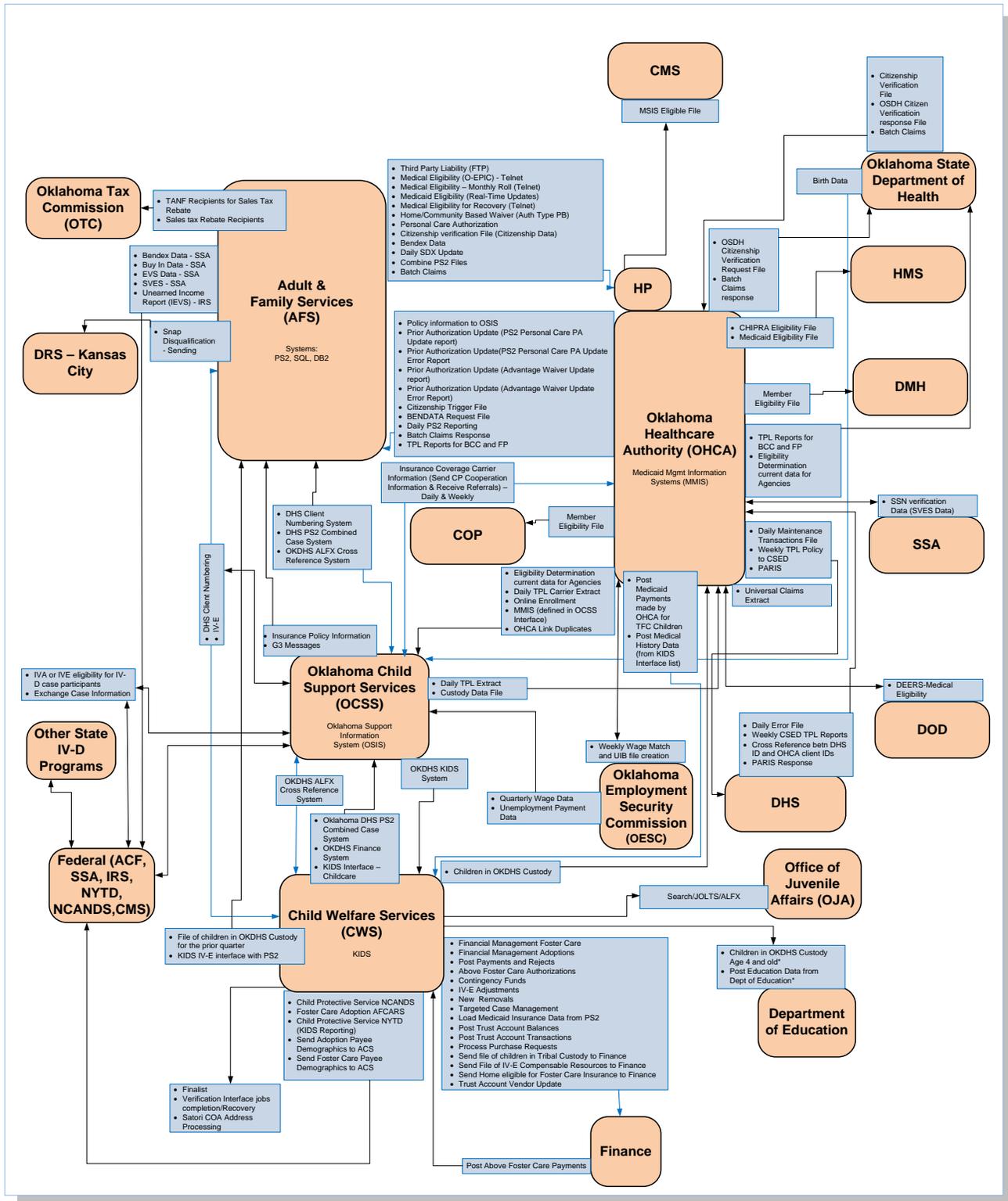


Figure 11: AS-IS System Overview/Data Exchanges

- 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 C.

4 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.

To accomplish this, governance requires organizational structure and processes and must identify who has authority to define and carry out its mandates. It must address the following questions:

- What decisions must be made to ensure effective management and use?
- Who should make these decisions?
- How will these decisions be made and monitored?
- How will these decisions be communicated?

The intent is to achieve goals, add value, and reduce risk.

The distinction with SOA governance is what things need to be governed when SOA is applied to our application portfolios. What are the extra things that have to be covered? SOA governance has to be in alignment with the rest of the governance in the organization including IT and Business governance.

4.1 AS-IS Governance

The current governance model consists of many groups each with a specific focus.

4.1.1 OKDHS – IT Governance Model

- **Purpose.** The Information Technology Portfolio Management Governance Board (IT Governance Board) is charged with reviewing, approving, and recommending for funding and resource level all information technology projects. Board members assess project technical validity and value, and ensure cross-division planning, scheduling, and compatibility of projects.
- **Membership.** The board is composed of 13 members appointed by the OKDHS chief officers are as follows:
 1. Chief administrative officer – two members
 2. General counsel – one member
 3. Chief financial officer – one member
 4. Chief information officer – one member
 5. Chief coordinating officer – four members
 6. Chief operating officer – three members
 7. Chief information officer
- **Bylaws.** The IT Governance Board adopts, alters, or amends bylaws that must be ratified by the Director and Chief Officers.

4.1.2 OHCA – IT Governance Model

OHCA currently chairs group meetings of a statewide HIE group to develop a state government exchange mechanism. This group consists of state health and human services agencies, including: OKDHS, OSDH, Oklahoma Department of Corrections, Oklahoma State Department of Mental Health and Substance Abuse, Vocational Rehabilitation, and Department of Insurance. In the future all of these entities will be involved in the statewide HIE governance committee.

OHCA is in the process of establishing an EA program. OHCA's current infrastructure has evolved over time without an EA program in place to guide design decisions or enforce standards. Some of the results of not having an EA program in place include tightly integrated monolithic systems, stop-gap business processes, redundant technologies and data fragmentation. The establishment of an EA program will begin the process of translating business vision and strategy into effective information technology services. The intent of the EA program is to provide direction and regulation of projects to ensure the reliability, interoperability and sustainability of systems used by OHCA. The value of the EA is realized through the creation and compliance with standards and guidelines.

CMS funds OHCA's projects, and wants to see progress in supporting the MITA architecture. OHCA has undertaken the effort of revamping business processes and replacing legacy technologies and applications with systems that will meet current and changing business requirements. The creation of an EA program is critical to the success of this effort. By creating MITA architecture and enforcing compliance to it, complexity and redundancy will be greatly reduced. Compliance with MITA will also facilitate the faster delivery of systems solutions and consistent planning and implementation across the enterprise.

4.1.3 OSDH – IT Governance Model

The OSDH IT Steering Committee Charter establishes the change control process for programs supported by the OSDH IT Infrastructure and Software Development Teams.

The scope of the OSDH IT Steering Committee is to review, prioritize and make recommendations on all IT infrastructure and development projects within OSDH.

The OSDH IT Steering Committee is responsible for the coordination of Infrastructure and Development project requests and their tracking process.

Some duties of the IT Steering Committee will include, but are not limited to:

- Annual Review of the IT Budget
- Review of Short-Term and Long-Term Equipment Replacement Plans
- Project Funding Impacts
- Outsourcing Recommendations
- Advise Senior Leadership on project developments that impact project scheduling and other programs within the OSDH

4.1.4 Overall Current Governance Structure

Figure 12 depicts the current governance structure of the agencies and business units involved in the scope of the interoperability effort.

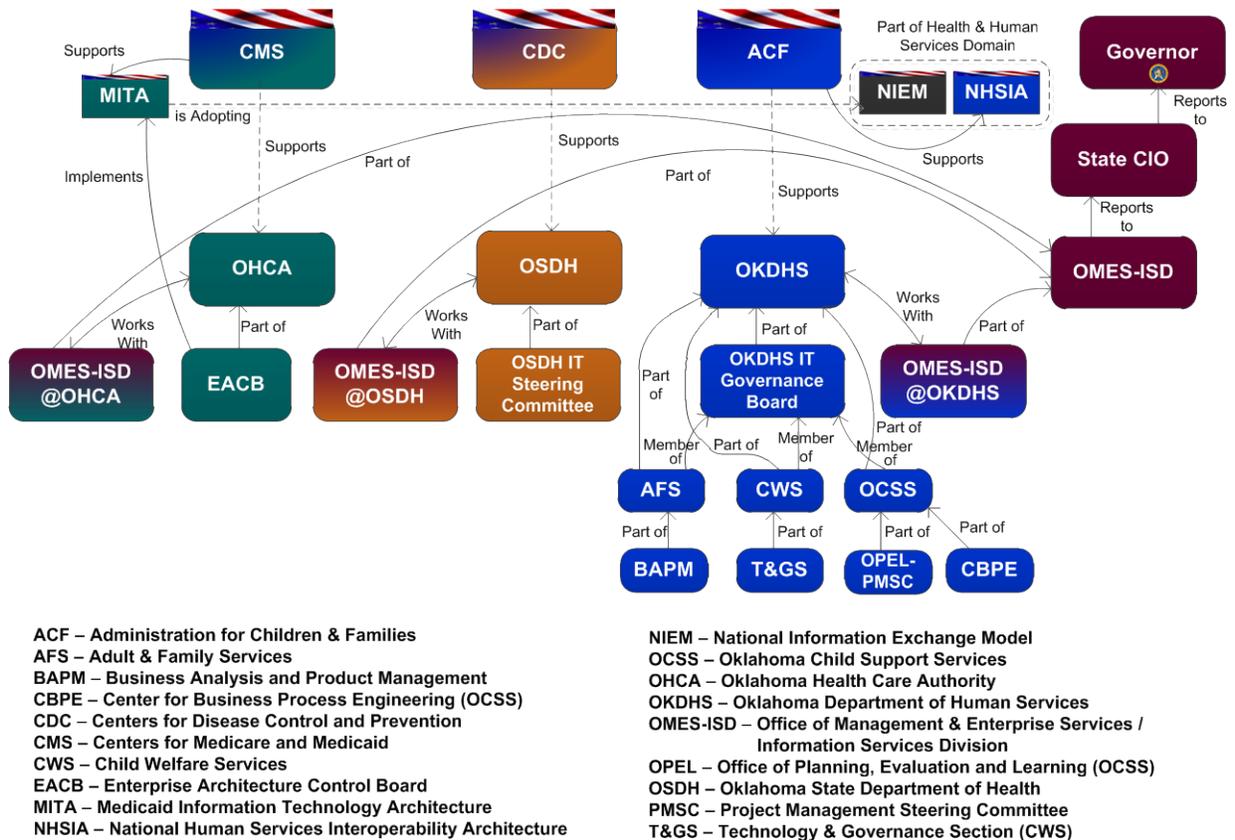


Figure 12: Current Governance Structure

4.1.5 State of Oklahoma – Enterprise IT Governance Model

From an enterprise or state-wide level, IT governance is vital to improve the effectiveness and efficiency of the State.

Figure 13 depicts a summary of the state’s enterprise IT governance structures. Although there are two structures, all the agencies involved with the interoperability effort and the SOA Roadmap will fall under the structure on the left of the figure below. Agency Executive Oversight will apply to all the agencies involved with the interoperability effort.

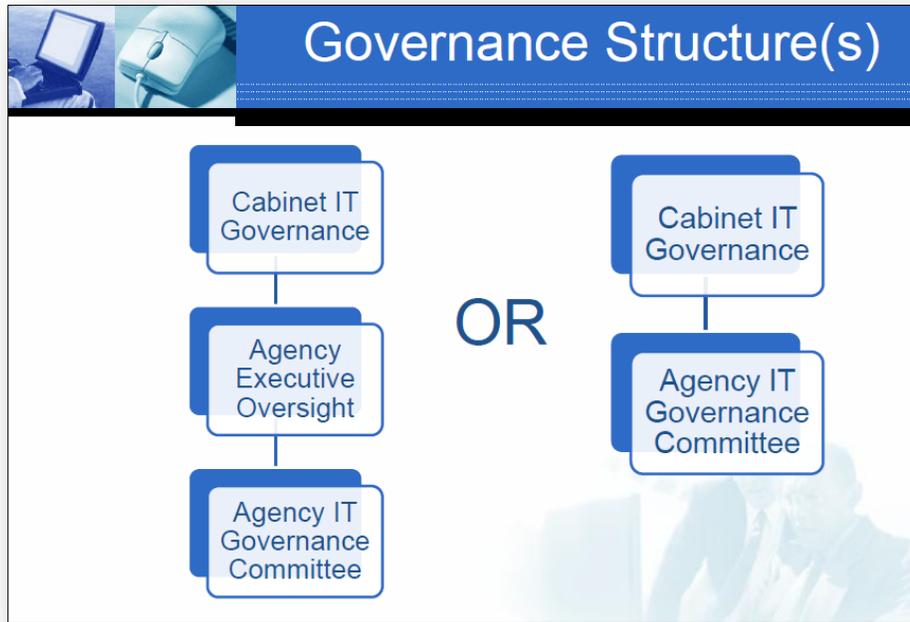


Figure 13: Governance Structure

Figure 14 below shows a hierarchical organization structure with the Governor establishing the overall IT guidance, the State Chief Information Officer (CIO) driving the execution of this guidance, and the IT service owners delivering day to day IT services to the State.

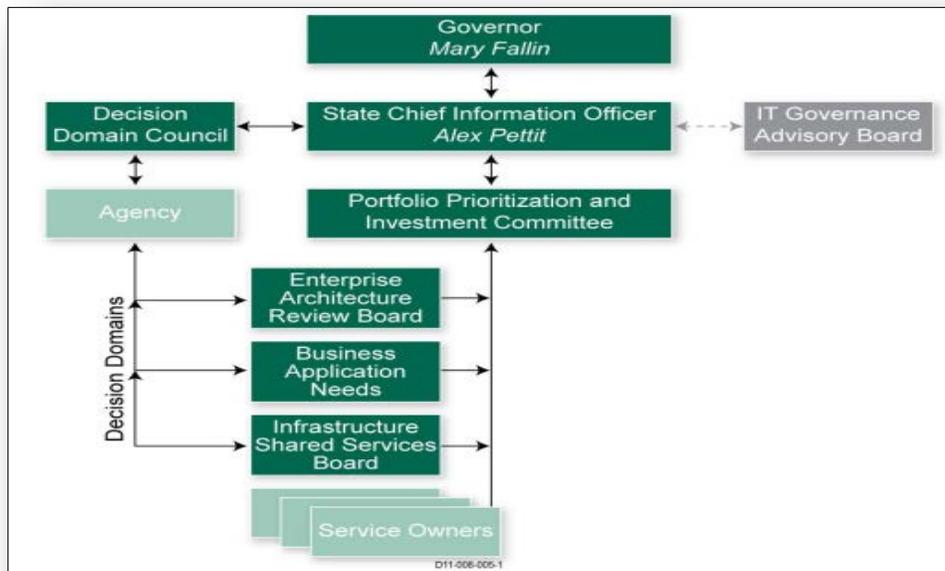


Figure 14: IT Governance Organizational Structure

The general governance model adopted by the state of Oklahoma for Enterprise IT Governance is depicted in Figure 15 below.

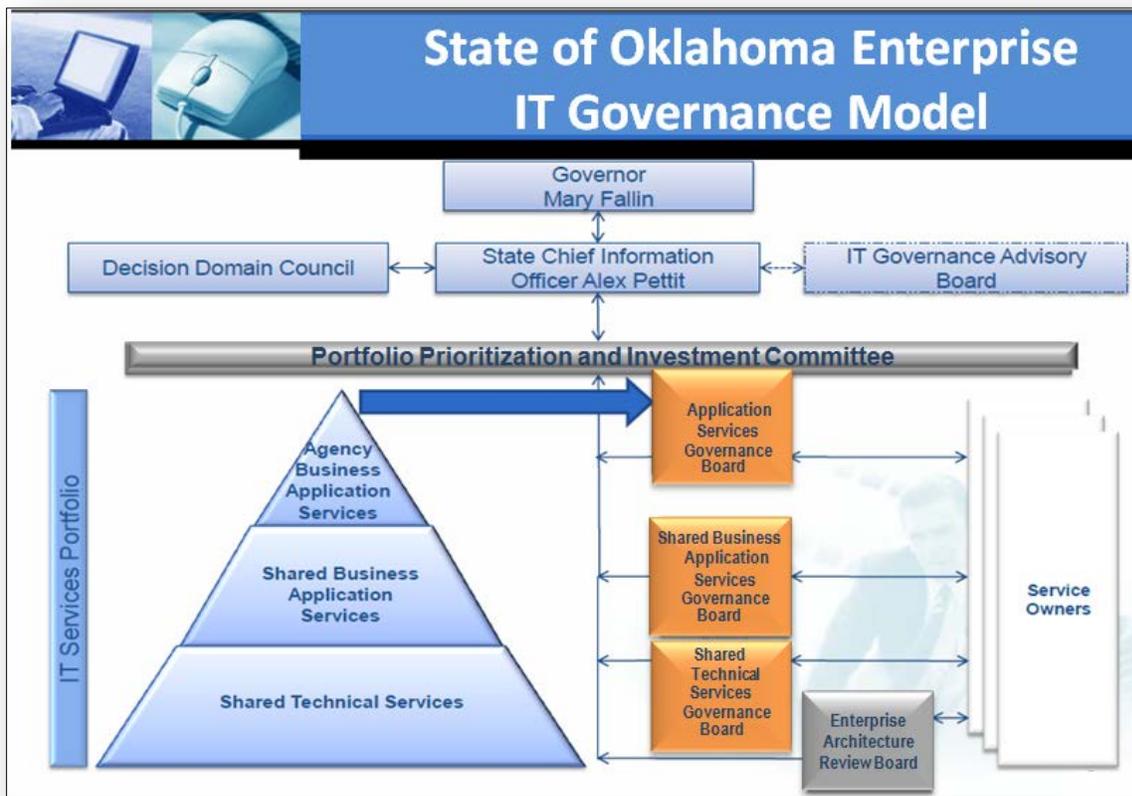


Figure 15: Oklahoma's Enterprise IT Governance Model

5 TO-BE SOA STRATEGY

5.1 TO-BE System Overview

The desired or TO-BE state is to have an environment characterized by interoperability. Interoperable systems share information and processes to efficiently deliver integrated services to the client community. Interoperability can be achieved via the design and implementation of an overall NHSIA Architecture, which defines the principles, standards, services, security, and interfaces to be followed by the component elements within the total system of systems. Figure 16 illustrates the potential TO-BE System.

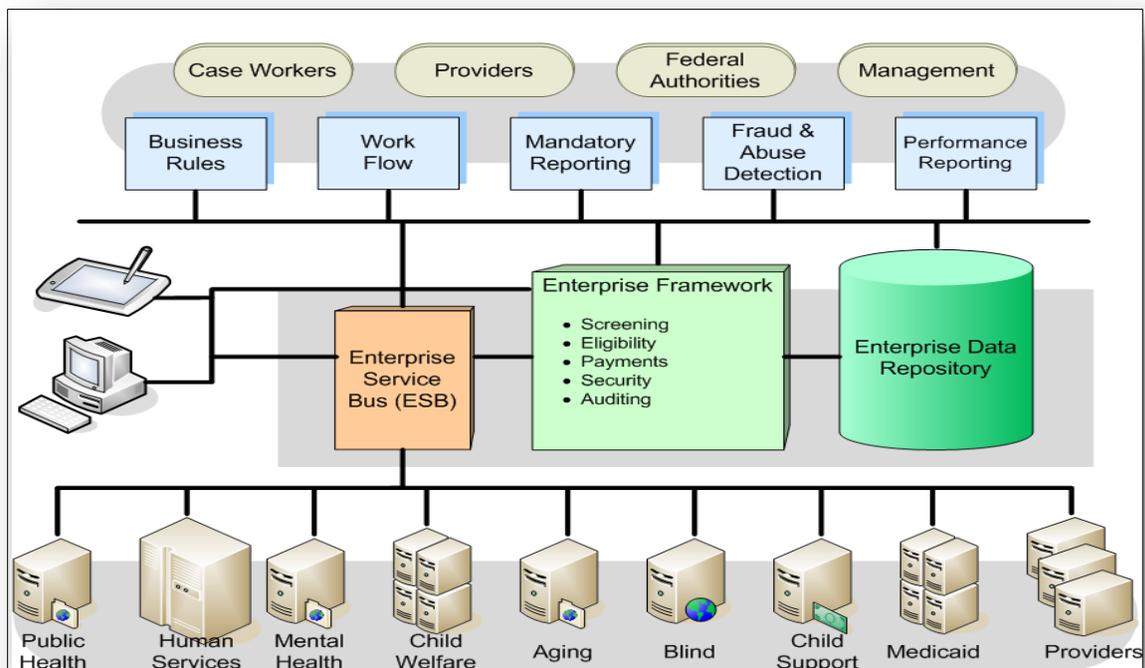


Figure 16: TO-BE Enterprise Architecture

In order to establish and adopt use of SOA, we need to define the detailed strategy for implementing SOA. At every step we should keep in mind the objectives of the SOA. Most, if not all of the decisions should be directly linked and justified against the SOA objectives.

The overall SOA Strategy will be derived from three strategic areas listed in the following steps:

- Step 1: Define the SOA Reference Architecture
- Step 2: Define the SOA Roadmap
- Step 3: Define the SOA Governance Strategy

Together these define the SOA Strategy. Although we define the SOA strategy in three steps, the suggested best approach is to run these steps in parallel or in an iterative fashion, feeding off each-other. For example, scoping the SOA initiative is part of the roadmap but should be the first activity, as it influences everything else. The roadmap should be driven in large part by the SOA reference architecture but should also consider the implementation of the governance strategy.

5.1.1 Step 1: Define the SOA Reference Architecture

The SOA reference architecture is, among the three components of the strategy, probably the easiest to define and most widely documented. Easiest because in IT we

are usually comfortable with working out architectures, most documented because most commentators of SOA have an architect background. In fact, most SOA initiatives – even the most technically and least strategically focused – probably have SOA reference architecture of one form or another.

Initially only general guidelines are included describing what we believe should be contained in the SOA reference architecture. This will evolve and become more defined as we work through the other interoperability project deliverables (web services, business processes, NEIM analysis, and eligibility workflow.)

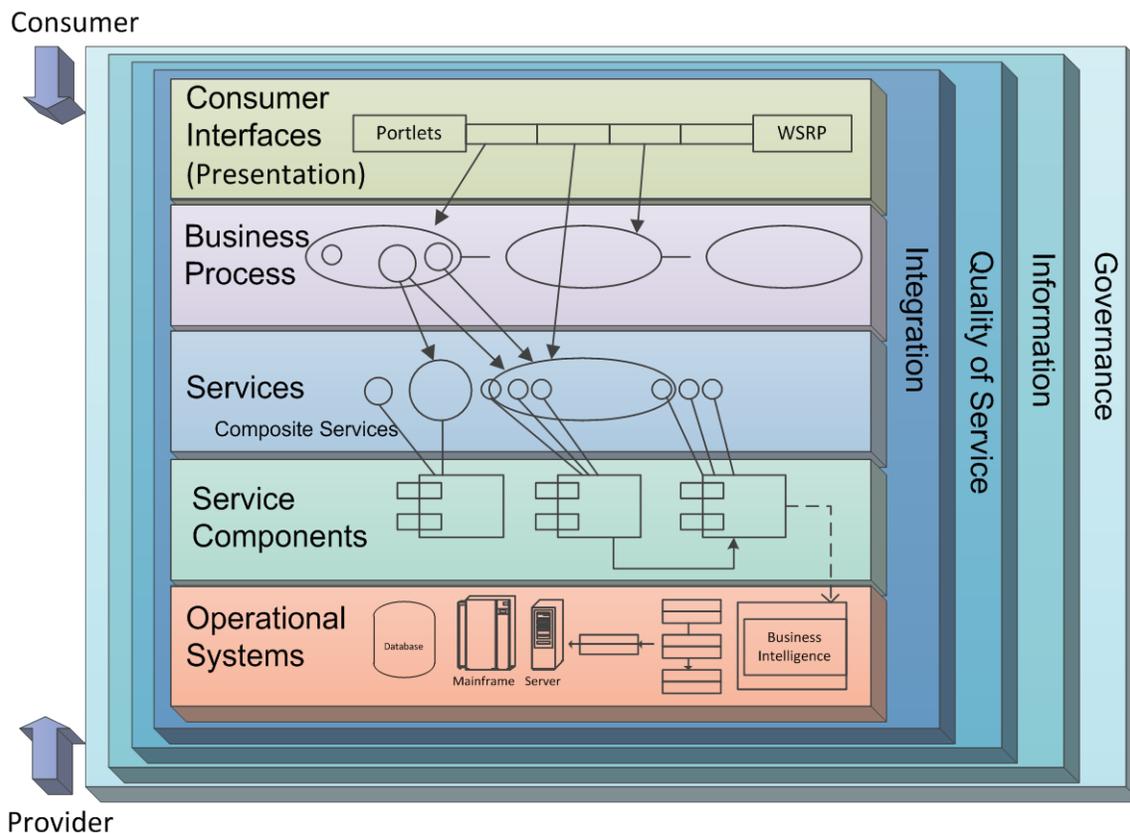


Figure 17: SOA Reference Architecture

This SOA Reference Architecture, as seen in Figure 17 is comprised of nine layers as follows:

- **Operational Systems Layer:** Programs and data of the operational systems of the enterprise. The new and existing infrastructure is needed to support the SOA solution.
- **Service Components Layer:** Software components, each of which provides the implementation or “realization “ for a service, or operation on a service, and binds the service contract to the implementation of the service in the operational systems layer.

- **Services Layer:** Services with their descriptions, contracts, and policies, and the containers that contain the service components.
- **Business Processes Layer:** Business processes and compositions in which business processes are composed of other business processes and of services.
- **Consumer Interfaces Layer:** The programs by which the users interface to the services.
- **Integration Layer:** Integration of and communication between other building blocks, including messaging, message transformation, complex event processing, service composition, and service discovery.
- **Quality of Service Layer:** Monitoring and management of the quality of service of the architected system, including its performance, reliability, availability, scalability, security, and manageability.
- **Information Layer:** Management, analysis, interpretation, and transformation of data.
- **Governance Layer:** Governance rules and procedures. Services and programs that support the application of the rules and the operation of the procedures.

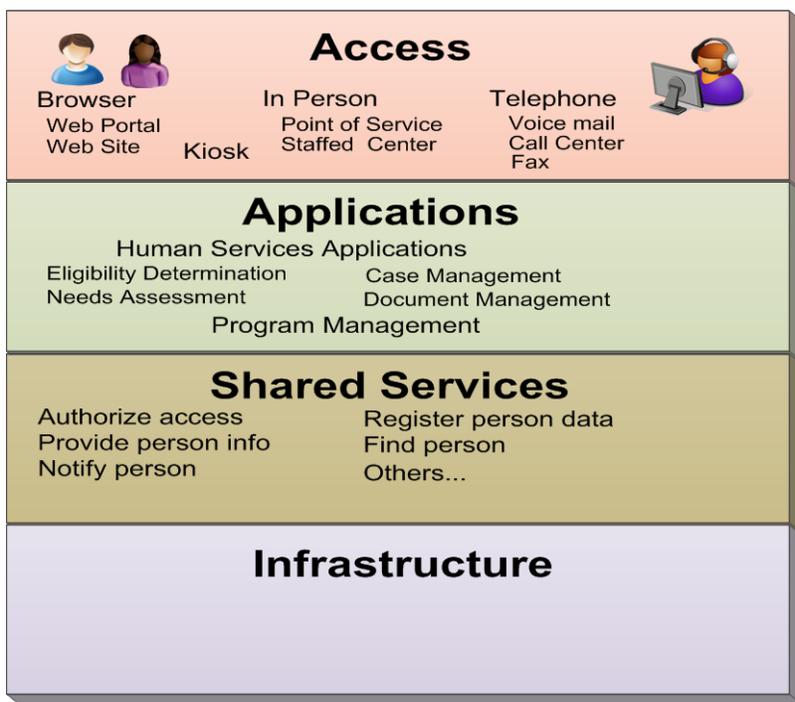


Figure 18: NHSIA Systems Reference Model Layers

The NHSIA Systems Reference Model Layers which are shown in Figure 15 include:

- **Access Layer:** The access layer includes components for presenting human services information and services to people, IT services for people, and traditional (non-automated) interactions with people. People may access human services (HS) information and services via electronic devices (computers, telephones, fax machines, or other). People may also interact directly with other people to access HS information and services.

Examples of components in the access layer include browsers, web portals, web sites, interactive forms, kiosks, telephone, voice mail, etc.

- **Applications Layer:** The applications layer includes high-level applications that normally support multiple human services domains, agencies, and programs. In this context an “application” is application software - a computer program designed for end users to accomplish specific tasks. What constitutes a “domain” depends on how the jurisdiction organizes its services.

Examples of components in the applications layer include human service applications that support multiple domains: eligibility determination, case management, and others. This layer also includes program management applications that support multiple programs: partner management, performance monitoring, and others. This layer may include applications unique to a domain, agency, or program (to meet unique requirements or because they are legacy applications). This layer may also include integrated applications (e.g., one application that handles eligibility determination and enrollment) to support multiple activities in one or more domains, agencies or programs.

Finally, this layer includes supporting applications such as rules engines, workflow systems, document management systems, and analytics packages. Applications should be interoperable so that users can easily accomplish all their tasks seamlessly.

- **Shared Services:** The shared services layer includes components that deliver functionally-oriented IT services and information (application services and data services) that are unique to the human services domains. Examples of shared services include updating information about a person or verifying credentials for a service provider. The information and information structures shared by multiple applications (e.g., master person index) also appear in this layer. “Wrappers” to enable legacy systems to discover and use shared services are in the shared services layer.

Examples of shared services are eMPI and legacy system “wrappers”.

- **Infrastructure:** The infrastructure layer includes IT services, systems, and data not unique to human service domains. This layer includes the tools for applications to discover and use the shared services.

The elements in the infrastructure layer include the ESB. Basic capabilities include mediation, routing, and data and protocol transformation. The layer includes a service registry and service broker functions. Elements in this layer include the commercial off-the-shelf IT services, hardware, and software that support all the upper layers.

Examples of components in the infrastructure layer include adapters, application servers, and data integration servers:

- ✓ SOA
- ✓ ESB
- ✓ Cloud Computing
- ✓ Infrastructure Security

- **Business Rules Engine:** Business rules engine is another component typically employed as a part of, or in conjunction with an ESB. A business rules engine is a software system that executes one or more business rules in a runtime environment. These rules will come from legal regulations, organizational policy, or other sources. A business rules engine enables such rules to be defined, tested, executed and maintained separately from application code. This provides a mechanism to adapt to changing rules without the need for major system updates.

A business rules engine typically includes a repository that permits rules to be externalized from application software. Most also include a rule definition tool that allows business experts to define and manage decision logic that was previously buried in software.

- **Services Registry:** A services registry is one of the fundamental pieces of SOA for achieving reuse. Typically a component of the ESB, it is a place in which service providers can document information about their offered services and potential service consumers can search for services. The reuse of services greatly depends on the ability to describe and publish the offered functionality of the services to potential consumers. A service registry organizes information about services and provides facilities to publish and discover services.
- **Architecture Drivers:** These architectural drivers influenced the development of the systems reference model and the identification of proposed applications and shared services. Architectural drivers are externally imposed authoritative mandates, policies, or conditions that strongly influence the development of NHSIA. These include:

- ✓ Achieve interoperability across programs and jurisdictions
- ✓ Architectural scalability to allow easy and rapid expansion to more jurisdictions
- ✓ Reuse processes, infrastructure, and systems by multiple programs and jurisdictions to reduce life cycle costs and share best practices
- ✓ Use COTS software to reduce life cycle costs
- ✓ Minimize life cycle cost, achieve a demonstrable return on investment (ROI)
- ✓ Information is maintained in multiple, geographically distributed, heterogeneous data structures
- ✓ Assure data privacy and confidentiality in compliance with government policies (e.g., HIPAA)
- ✓ Leverage Federal investments in health care (e.g., as a result of the Patient Protection and Affordable Care Act (PPACA))

5.1.2 Step 2: Define the SOA Roadmap

The SOA Roadmap defines the steps the enterprise will take in the next few years for implementing the SOA Strategy and achieving the SOA benefits.

It should not include every detailed step for the length of the roadmap as it would be very time consuming to define and in all likelihood it would be wrong the minute you start the implementation. Instead, pragmatism should guide you here: the roadmap should be very clearly defined for the first few months and more and more open the further in time it gets.

As with all the elements of SOA strategy, the roadmap should also be a living document that is refined and updated as you go along, but which helps you make sure you don't miss any important steps.

Ideally you should represent the roadmap graphically to ease communication to, and achieving buy-in from key stakeholders, including IT management.

Short Term

For the first few months, the roadmap should include the one or two projects that you have chosen to first implement SOA, or if SOA has already been used, where you will first apply your new SOA strategy. It should also define to what extent the governance strategy and the reference architecture will be implemented – remember to be pragmatic: focus on the easiest parts that will bring you the most benefits. You may also want to include one or two of the riskiest aspects of the strategy so that they can be tried out and de-risked.

Mid to Long Term

Longer term, the roadmap should specify when and in which order all the aspects of the strategy should be implemented.

An example item on the roadmap might be one element of the infrastructure. Perhaps a service security gateway for exposing services to partners. The trigger or target is not necessarily a specific date: it could be dependent on other factors such as when a certain number of services are exposed to partners. It helps however to estimate a date for when this trigger should be reached.

It might also include when the platform or the SOA is rolled out to different business units or agencies for adoption.

SOA Objectives

Ideally you should also include in the roadmap when you expect to reach certain target objectives of your SOA. For example if one of your objective is "reduce partner onboarding time", you should specify when it would be reduced by say 20%, 40% and 60%, based on how the key systems that are integrated with partners are SOA-enabled.

5.1.3 Step 3: Define the Governance Strategy

An important part of the strategy describes how you will govern your SOA. Without governance, you will likely not follow your SOA reference architecture, your SOA roadmap will falter and ultimately you will not achieve your SOA objectives.

A governance model for SOA must be put in place to achieve true interoperability. Governance is about providing guidance for decision-making. Governance defines the principles for making decisions when executing SOA. Some type of SOA Governance Council must be established to guide sharing at both the data and web services levels, and achieve a cross-organizational consensus and understanding at the workflow or business process level.

Since SOA is a highly shared environment, it is critical that the SOA governance model be defined and implemented to manage an environment that is acceptable to all stakeholders. Standards must be set and policies determined for how services will be created, certified, modified, and retired as well as how security will be defined and enforced. Initial and sustaining funding models and the mechanisms to implement SOA infrastructure must be agreed upon.

Figure 19 is a high-level view of how SOA governance extends and supports both enterprise architecture and IT governance.

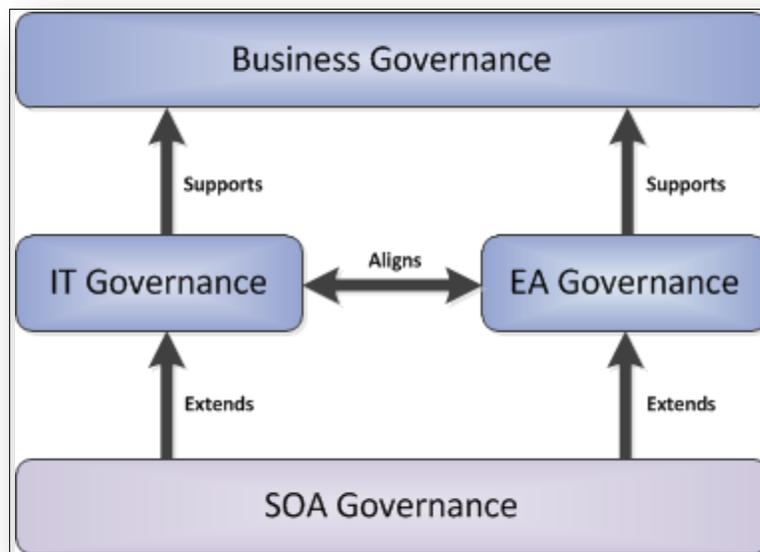


Figure 19: SOA Governance IT and Enterprise Architecture Governance

Typically, an SOA governance group consists of representatives from Enterprise Architecture (EA, the different lines of business and finance. Failure to address organizational and change management issues will lead to slow SOA adoption that lacks coherence, because employees aren't empowered (through organizational structure, training, and incentives) and aren't held accountable for delivering on SOA benefits.

An interagency governance team must work together to create rules for quality data being exchanged and accountability between agency's hosting and exchanging data. The philosophy and level of data governance must be agreed upon by the interagency team to ensure valid, current and secure data. The data must be shared using a national common format as NIEM. The governance of data must meet Federal and state policy regulations.

Some of the typical SOA governance decisions to be made in each SOA initiative are:

- Which Services are needed?
- Which Services shall be implemented first?
- Is this really a new, reusable service?
- Who pays for the development and maintenance of the service?
- Who owns this Service?
- Who approves changes to existing services?
- How do proposed and approved changes to existing services impact its current consumers?

Figure 20 shows where SOA Governance may fit in the State's Enterprise IT Governance Model.

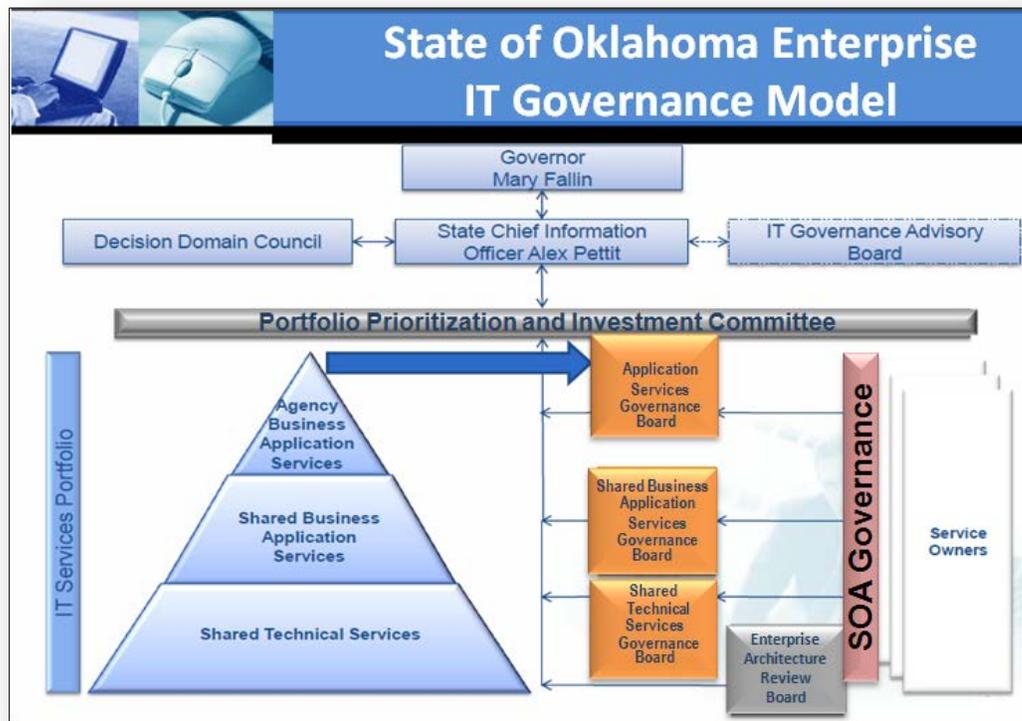


Figure 20: SOA Governance with the Enterprise

NHSIA Governance

ACF suggests that each state undertaking NHSIA may want to establish a NHSIA program management office to manage the effort. If there is a governance structure for enterprise-wide architecture activities, NHSIA should fit into that structure. If there is no governance established for activities that address the enterprise as a whole, then the NHSIA program manager may establish a governance structure for NHSIA. Essential elements of a governance structure focused on NHSIA would include:

- **Executive Steering Committee (ESC):** This should include the executives of the primary agencies that provide human services. This committee establishes top-level policies and priorities for the program and architecture. The ESC approves strategic plans and budgets.
- **NHSIA Program Manager (PM):** The NHSIA PM has the responsibility for planning and executing the program.

- **NHSIA Chief Architect:** The chief architect is responsible for the technical aspects of developing and maintaining NHSIA.
- **Architecture Configuration Control Board (ACCB):** The ACCB has representatives from each major stakeholder group. They are responsible for reviewing proposed changes to the architecture, recommending approval or rejection to the NHSIA PM, and ensuring that changes are properly incorporated into the architecture.
- **Architecture Staff:** The architecture staff supports the chief architect in developing and maintaining the architecture.
- **Policies and Procedures:** A set of governance, compliance, and usage policies and procedures is necessary to define the roles and responsibilities of each of the NHSIA stakeholders.

5.2 TO-BE Security Requirements

Securing open, loosely coupled systems in an SOA requires a much more sophisticated security approach than traditional distributed computing architectures, involving multiple administrators that support distributed users. Different systems now have different policies and possibly different security mechanisms. As a result, administrators within the enterprise must manage security much more actively than was necessary in the closed, "islands of security" model. In addition, enterprises should centralize their administration capabilities, and implement a hierarchical, delegated administration model to maintain a coherent, yet scalable enterprise security policy. Likewise, when organizations seek to work together in a trust relationship, they must federate their enterprise identity management capabilities. Such federation can both take advantage of SOAs within the participating organizations, and also forms an essential prerequisite for extending SOAs beyond the edge of the enterprise. As shown in Figure 21 below.



Figure 21: Identity Management & Access Control

Many security technologies, models and systems have been developed for SOA, covering one or a combination of security aspects such as authentication, authorization, encryption, trust, confidentiality or access control.

Authentication proves that the requestor of the service is who they claim to be. The authentication service may be one that supports some type of identity management service.

Authorization determines the set of services the user is entitled to use. Typically, authorization will be based on several dimensions such as user's role or type of user (employee, contractor, vendor, etc.).

Access control determines which functions and data within a service the user is entitled to use. These will be a set of specialized services that allow a user access to specific functions, like the ability to edit, update, or delete given data or content.

Privacy & Integrity within SOA security utilizes privacy (encryption-decryption) and integrity (signature-verification) for information in motion as well as information at rest. Through Secure Sockets Layer (SSL) the transport layer is secured, whereas messages using Web Services (WS)-Security standards, Simple Object Access Protocol (SOAP) and Extensible Markup Language (XML) are encrypted and signed granularly at the content-level. The combination of transport-level and content-level privacy and integrity provides significant control for companies to implement their security policies. With such flexibility, the burden of testing possible variations in the standards used, as well as the content over which the privacy and integrity policies are implemented, is now the responsibility of the quality assurance and security team within the organization.

5.2.1 Policies and Procedures

- Safeguards must be designed to prevent unauthorized access and use.
- Must adhere to established policies, procedures, rules and regulations (e.g., IRS Publication 1075, HIPAA, etc.)

5.2.2 Web Services Security

The following table represents a snapshot of the current specifications relevant to security in the web services space. The issues with these specifications, apart from the web of relationship between these specifications and between them and the base W3C and OASIS XML specifications, is that they are complex and are evolving.

Table 5: Web Services Security

XML	Messaging	Security	Related
XML	SOAP	XML Encryption	WS-Policy
XML Namespaces	MTOM (Attachments)	WS-Security	WS-PolicyAssertions
XML Information Set	WS-Addressing	WS-SecureConversation	WS-PolicyAttachment
XInclude	WS-Routing	WS-Trust	WS-SecurityPolicy
Xpath		WS-Federation	
		WS-Federation Active Requestor Profile	
		WS-Federation Passive Requestor Profile	
		Web Services Security Kerberos Binding	
		Web Services Security Addendum	

Security standards for external web applications exist for OKDHS. All new web applications, created after 4/1/2012, that require external users to log in must use the OKDHS Enterprise Portal for registering users, maintaining credentials, resetting passwords, requesting and receiving access to secured web applications. Typically users register themselves, and request access to applications. It is recommended for current web applications that use another login, to be converted to use Enterprise Login when it makes business sense to do so.

All web applications that require external users to log in must use the OKDHS Enterprise Single Sign On (SSO) when logging in to the application as defined in the documentation for Enterprise Login. This documentation is available in the OKDHS Application Documentation shared folder under Global Modules.

Security for Internal Web Applications: All internal .NET applications will use Integrated Windows Authentication using the user's OKDHS user ID and Active Directory security groups.

Internal users must not be required to log in to an application after logging in to their Windows machine.

An application needing to authorize access to secured areas within the application must use Active Directory groups to do so.

All internal .NET web applications needing to restrict access will use the Enterprise Security Module. The Enterprise Security Module (aka Global Security Module) provides ASP.NET Intranet applications with the ability to perform security access management. This module must be used by all internal OKDHS .NET web applications that have security requirements that include authentication and/or authorization. Any enhanced authorization requirements that cannot be provided by Enterprise Security Module must be developed with the approval of the Enterprise Architecture & Engineering Services (EAES) unit.

5.2.3 Security for Web Services and Windows Communication Foundation (WCF) Services

Web services and WCF services that are not for public consumption must take precautions that prevent unauthorized applications from calling them.

Any Web/WCF Service that is not meant for public consumption must have security to restrict access to authorized users and/or applications. The EAES unit will provide guidance on how to implement said security.

Web/WCF services must live on an internal web server. If they need to be accessed from the outside, they must be accessed by a web application that lives in the DMZ. If a need for a public-facing Web/WCF service arises, it must be discussed with and approved by the EAES unit. EAES will collaborate with the appropriate project team members to plan for how this should be done in a secure manner.

SSL/Transport Layer Security (TLS) must be used on all web applications and web/WCF services that are transmitting secure data, whether internal or external.

Any other Web/WCF service security methods must be approved by the EAES unit before use.

5.2.4 Security for Databases

Web applications or web/WCF services that access databases have the responsibility to verify that the person accessing the data has the authority to do what they are asking to do. The database will be accessed by the application using a proxy ID after the application has verified the request is authorized.

Databases that need to be accessed by web applications in the DMZ must live inside the OKDHS network and be accessed by an internal web or WCF service that is called

by the web application. In addition to the web application determining if the user has access, the internal web/WCF service will perform its own security to make sure the application calling is authorized to call it.

5.2.5 Exceptions

Exceptions to this standard must be approved by the EAES unit. Any dispute regarding an exception request should be escalated to a Data Services Division (DSD) Director. This standard applies to COTS products but exceptions for these will be evaluated on a case-by-case basis.

5.3 TO-BE SOA Interfaces

User interfaces should be componentized. While it is permissible to have multiple types of user interfaces to interact with (i.e. multiple browser views customized for the users' needs, Wireless Device Markup Language (WDML)/Wireless Markup Language (WML) views, e-mail, etc.), the common user interface barrier seen between applications should be eliminated. Every OKDHS worker should simply have a portal-like ability to see all the data they need to do their job without manually going to different websites or opening other applications. The fluidity should ultimately make it unknown to the user that the applications or the sources of data they are interacting with in the backend are different.

Similarly, interfaces for external OKDHS clients should be designed from the same perspective – whether they are web sites, kiosks, email based, or phone based Interactive Voice Response (IVR) systems, they should be accessing the same middleware components and be reusable.

User Interfaces in the TO-BE system are somewhat dependent on the design of the services and how they plan to be implemented. Some of the current user interfaces might remain as they are right now, or may be modified and new ones might evolve. Choices that we make also depend on the technology that we will be using in the TO-BE System. New technologies will impact the way the exchanges are handled.

Using MDM to store master data will change the way the stakeholders handle the data exchange because it changes the process of exchange and service delivery. User interfaces might be impacted due to the way the exchanges will be handled.

5.3.1 SOA and the Enterprise Service Bus (ESB)

There is no universal definition of Enterprise Service Bus. Vendors define the term differently according to their own market in such a way that they are the only vendor that has a product that meets their definition. The only similarity between all of the vendors' ESB implementations is that at least part of it is based on Message Oriented Middleware. OKDHS' application architecture supports the concept of a messaging layer, but currently has no specific product that performs this function.

5.3.2 Message Oriented Middleware (MOM)

Message Oriented Middleware (MOM) is a category of inter-application communication software that generally relies on asynchronous messaging passing as opposed to synchronous request/response.

Most MOM depends on a message queue, although some implementations may also use broadcast or multicast technology. OKDHS's Enterprise Application Architecture supports a distributed MOM implementation called a bus.

5.4 TO-BE Web Services

OKDHS supports the use of web service standards. The use of basic web services standards gives the enterprise one of the best ways for multiple applications to reuse code. The nature of a basic web service is:

- Has directed one-to-one bidirectional request/response connections
- Has flow routing that is directed by the client (sender) in a "find-bind-invoke" fashion
- Employs a linear path of execution through a hierarchy of modules
- Is closed to new, unforeseen input once a flow is started

There are three main areas for the use of web service technologies at OKDHS:

1. As a communications mechanism for entities external to OKDHS' network to interact with OKDHS applications
2. For making application components available for cross platform reuse within the enterprise
3. As a communications mechanism between different layers running within different containers.

Each of these three areas has different needs and goals that will affect the design. Web services are not a "one size fits all" with regard to design, use, and implementation.

- **As a communications mechanism for entities external to OKDHS' network to interact with OKDHS** - In this case, the use of the web service is viewed as a gateway to OKDHS so using the most popular standards are of the highest priority. The most popular standard, SOAP (over HTTP), was designed for this kind of use. The intent of these kinds of web services is that they are called infrequently (i.e. low volume of calls).
- **For making application components available for cross platform reuse within the enterprise** - SOAP is a heavyweight protocol. It uses a large and complex XML envelope and is up to ten times slower than binary network protocols like RMI or IIOP. For this reason, it may not be the best standard for

frequent conversations within the enterprise. If performance is an issue, other standards may need to be substituted. The use of REST (Representational State Transfer) may be used as an alternative.

- **As a communications mechanism between different layers running within different containers** - There are some frameworks that will take well-designed layered code and generate the client and server side code that will be executed in different physical tiers. Generally this kind of use of web services does not use standard protocols because of the overhead. Highly efficient code is more important than the standard in this case because the framework is generating the skeleton and stub code. The developer never directly interacts with the generated web services code directly.

6 RECOMMENDED APPROACH

6.1 The SOA Roadmap

The SOA Roadmap is based on several reviewed SOA Methodologies, SOA Maturity Models and the current SOA Maturity within the state. Most agencies have little to no SOA.

This SOA Roadmap indicates the typical SOA initiatives that need to be performed to increase the level of SOA maturity within the organization. The initiatives indicated are based on the Maturity Levels of the SOA Maturity Model, and the deliverables and focus areas indicated in the SOA Methodology.

6.1.1 Construct and Maintain Master Services Portfolio

As part of implementing SOA, it is recommended that service portfolios or a Master Services Portfolio be established where all defined business and IT services can be tracked. This service portfolio(s) will enable the reuse of services already designed, and further enhance standardization of services across the enterprise.

Once these business and IT service repositories have been defined an applicable software development lifecycle (SDLC) should be updated to ensure that during the solution design and development phases the business analysts and developers query the service portfolio(s) to identify and reuse existing services if possible rather than unnecessarily duplicating functionality and services.

6.1.2 Implement Cross Enterprise Security

As the institutionalization of SOA enabled business processes matures the management of security across these more agile business processes becomes a critical factor.

It is suggested that the state embark on a cross enterprise security initiative to ensure that security and access control relating to at least the SOA business processes and enabling systems can be managed centrally.

The establishment of cross enterprise security will enable the state to deploy agile business processes with more ease and in less time. The establishment of cross enterprise security will also reduce the amount of time and effort that needs to be spent on user account maintenance especially relating to the various enabling systems (often legacy) that users need access to when they are granted access to a business process. Cross enterprise security allows the organization to make the concept of “single sign on” a reality.

6.1.3 Extend the Scope of SOA Solutions to Span Multiple Business Units

Start simple then increase complexity as SOA efforts mature. As SOA maturity increases and SOA capabilities are established the state should engage in more complex SOA projects spanning multiple integrated applications across multiple business units.

It is important to ultimately engage in the more complex projects as they typically involve complex business processes that can deliver considerable benefit to the organization when supported by SOA principles and architecture resulting in agile business processes.

6.1.4 Extend the Scope of SOA Solutions to External Business Partners

Several of the agencies' business processes span both the agency and their business partners.

Once the SOA maturity has reached a level where substantial benefit has been realized from the institutionalization of SOA internally to the organization, it is recommended that the agency extend the scope of the SOA initiatives to include business processes spanning both the agency and their external business partners. An obvious prerequisite for this expansion is that their business partner(s) needs to be able to provide the required technical and business services to enable the multi-organizational business processes.

6.1.5 SOA Communication and Update of Applicable Knowledge Portal

In order to ensure that the Business and IT stakeholders of the organization are aligned in terms of the goals and objectives of the SOA program, it is critical that an Enterprise SOA Strategy be formulated and agreed by the business and IT stakeholders involved. It should be noted that the required strategy is an enterprise strategy, and should span the strategic objectives for SOA across the entire enterprise, not only selected business units.

Once the Enterprise SOA strategy has been agreed it should be communicated to the organization. This will ensure that a common vision and mission for the SOA exists within the organization, and that no rumors regarding the SOA program derail the program. Further, the ongoing communication of SOA related initiatives and the progress towards higher levels of maturity is critical to the success of SOA adoption in the state. Knowledge portals or information sharing sites such as SharePoint sites or the InfoNet portal is an ideal mechanism for knowledge sharing, but should not be the only method of communicating with the rest of the business.

6.1.6 Develop Target Enterprise SOA Architecture

A high level target Enterprise SOA Architecture should be developed based on a SOA Reference Architecture. This architecture should consist of the fundamental SOA components, these fundamental components typically includes the following:

- Communication Backbone
- Business Process Management Application(s)
- Business Services Portfolio
- Technical Services Portfolio
- Business Rules Engine
- Data Warehouse
- Web Portal

The target SOA architecture does not need to be a logical architecture of the entire SOA solution, a conceptual view of the SOA architecture is sufficient at this stage, provided that the conceptual architecture includes all the fundamental SOA components and indicates their interaction between the components on a conceptual level.

Added a new line here

6.1.7 Specify SOA Policies and Procedures

In order to ensure the successful establishment of the SOA architecture, enterprise SOA policies and procedures need to be developed. These policies and procedures are required to guide and govern the design, development and deployment of SOA in the organization. One of the key enablers of a successful SOA architecture is the standardization of SOA components to encourage and enable reusability. Enterprise SOA policies and procedures are required to enhance the standardization of SOA components, and ensure that a common approach is used across the enterprise to realize the target SOA architecture.

6.1.8 Integrate SOA Principles into Organization Wide SDLC

To ensure that the SOA program is delivered consistently across the state, it is important to amend the existing SDLC within the state to include SOA principles.

The enhanced SDLC should include SOA principles enforcing event driven design, reusability of SOA components, standardization, flexibility and the registration of business and technical services in the services portfolios.

The SOA principles that need to be integrated into the existing SDLC should influence the design, develop and deploy phases of the existing SDLC, and should ensure that the revised SDLC is aligned to the enterprise wide SOA policies and procedures.

6.1.9 Develop and Implement SOA Lifecycle Governance

The establishment and implementation of SOA lifecycle governance is critical to ensuring that the design and development of new and changed applications are aligned to the SOA strategy and SOA architecture as defined by the organization, and adheres to the SOA policies and procedures developed by applicable governing entities.

SOA lifecycle governance should be tightly integrated throughout the entire SDLC, and various “gate-reviews” should be introduced into the SDLC to govern the design and development of solutions based on the SOA strategy, architecture, policies and standards.

6.1.10 Summary of SOA Governance Strategy outlined earlier:

- Establish governance to support interoperability
- Establish an Interagency Steering Group (OKDHS, OSDH, OHCA, etc.)
- Resource an Interoperability Program Office
- Policy and technology standards for data stewardship, security and consent
- Seek clarification on federal and state confidentiality rules so information can be shared and used more effectively
- Leverage basic building blocks for interoperability including: the Health and Human Service NIEM Domains, MITA, and NHSIA

6.1.11 Ensure Ongoing Partnership between IT and Business

The SOA program is an organization wide program, and should be perceived as one by the entire organization. As previously noted, the program should not be driven purely from an IT or Business perspective, but should be a joint effort from both Business and IT. It is of the utmost importance that employees of the organization perceive the program as driven from both a Business and an IT perspective to ensure that the program receives the required support.

The primary objective of the SOA program should to enable the IT organization to support business processes in an agile and cost effective manner, and this objective cannot be achieved without the full support and involvement of both business and IT stakeholders.

6.1.12 Ensure Executive Commitment and Sponsorship for SOA Program

In order to illustrate the organizational commitment to the SOA program, visible executive commitment and sponsorship is required. Without visible executive commitment, the program can be perceived as a trivial exercise, and the program will be at risk of not receiving the required support from a prioritization perspective. If the program is perceived as being trivial by the stakeholders within the organization it will be extremely difficult to execute the program successfully.

6.1.13 Provide SOA Training and Certification

In order for the adoption and implementation of SOA to be successful, it is essential that SOA training be provided to employees. The SOA training provided will differ from user training, enabling users to utilize the new functionality provided by SOA applications to event driven design training to enable business analysts and developers to better design and develop SOA applications, and adhering to SOA design standards when designing and developing new solutions.

6.1.14 Monitor and Report on Service Performance

Throughout the execution of a SOA program at the state of Oklahoma it is important that the benefits realized by SOA be illustrated to all stakeholders involved. This will assist the SOA program in retaining momentum, stakeholder buy-in and may also assist in securing funds for the future execution of the program.

OHCA has already begun SOA implementation, process automation and the implementation of associated services. A key element of defining service specifications is the definition of service levels and expected performance metrics. These service levels and performance metrics are being defined as part of the implementation of processes and services. However, the next step is to monitor and report on the performance of these services, and to identify potential areas for improvement.

6.1.15 Implement Services Using ESB

Oklahoma should continue migrating business processes to the SOA architecture as they are currently doing. The complexity and scope of business processes migrated should gradually be increased as the SOA capabilities within the organization mature. Enterprise service bus (ESB) is a good choice for service enablement if the application you're trying to enable provides an interface to connect it to other systems. A good ESB provides all the tools you need to build XML services that leverage those APIs

6.1.16 Potential Sequence of SOA Initiatives

The initiatives described above can potentially be sequenced as indicated in Figure 22 below.

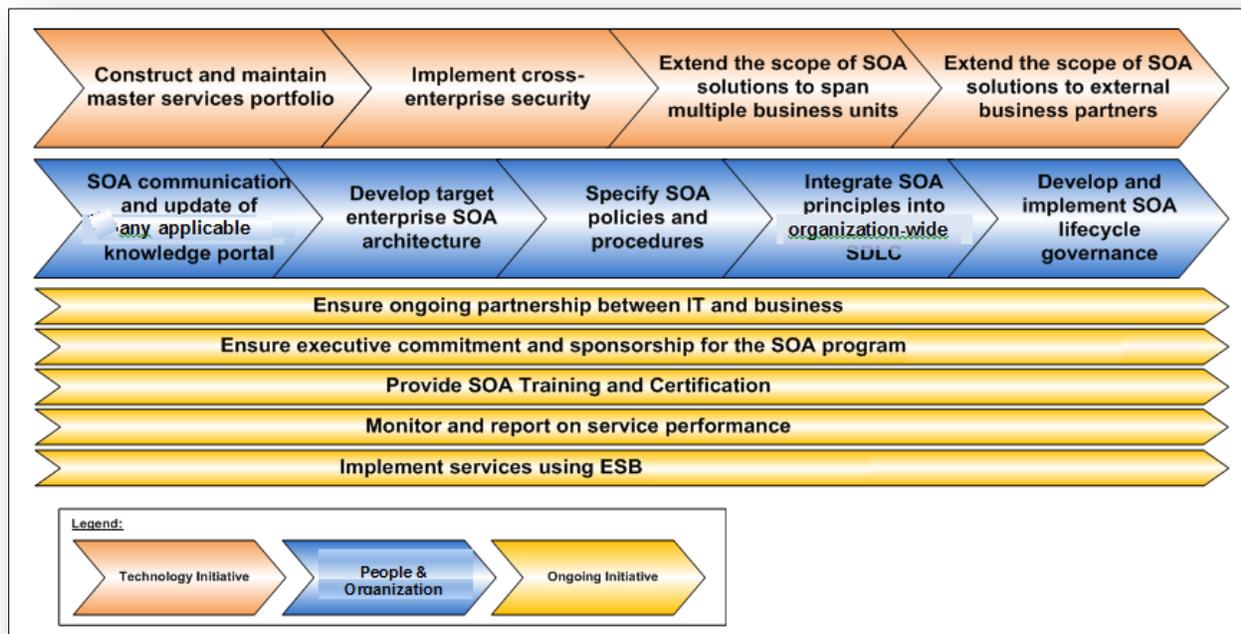


Figure 22: Potential SOA Initiative Sequence

6.2 Summary

The SOA roadmap refers to certain initiatives that are already underway between OKDHS, OHCA and OSDH, but largely provides guidance for new initiatives that should be executed to enhance the maturity level of SOA within the state.

The initiatives indicated in the roadmap above should not be viewed as the only SOA initiatives that should be executed by agencies of the state of Oklahoma to increase the SOA maturity in the organization. These initiatives are the key SOA initiatives that need to be executed, but not the comprehensive list of initiatives and the roadmap provided should be used as guidance to mature SOA at the state.

In parallel with the initiatives mentioned in this roadmap Oklahoma should continue gradually implementing business processes following the SOA guidelines and principles as they are currently doing.

The complexity and scope of the business processes migrated to the SOA architecture should gradually be expanded to incorporate multiple integrated applications spanning multiple business units and thus proving benefit to multiple stakeholders of the SOA program.

7 ACRONYMS

Acronym	Definition
ACA	Affordable Care Act
ACCB	Architecture Configuration Control Board
ACF	Administration for Children and Families
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
CHIP	Children's Health Insurance Program
CIDS	Case Information and Data System
CIO	Chief Information Officer
CMS	Centers for Medicare and Medicaid Services
CSENet	Child Support Enforcement Network
CWS	Child Welfare System
DB	Database
DDSD	Departmental Disabilities Services Division
DOD	Department of Defense
DoDAF	Department of Defense Architectural Framework
EA	Enterprise Architecture
EAES	Enterprise Architecture & Engineering Services
EDI	Electronic Data Interchange
eMPI	Enterprise Master Person Index
ESB	Enterprise Service Bus
ESC	Executive Steering Committee
FACS	Family Assistance/Client Service
FEA	Federal Enterprise Architecture
FIDM	Federal Institution Data Match
FTP	File Transfer Protocol
GFIPM	Global Federated Identity and Privilege Management
GRA	Global Reference Architecture
GUI	Graphical User Interface
HIE	Health Insurance Exchange
HIPAA	Health Insurance Portability and Accountability Act of 1996

HNC	Healthcare Network Cloud
HPES	Hewlett Packard Enterprise Service
HS	Human Services
HSA	Health Services Application
IO	Insure Oklahoma
IPHIS	Interoperable Public Health Information System
IRS	Internal Revenue Service
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
MDM	Master Data Management
MITA	Medicaid Information Technology Architecture
MMIS	Medicaid Management Information System
MOA	Memorandum of Agreements
MOM	Message Oriented Middleware
NASIRE	National Association of State Information Resource Executives
NCANDS	National Child Abuse and Neglect Data System
NHSIA	National Human Services Interoperability Architecture
NIEM	National Information Exchange Model
NYTD	National Youth in Transition Database
OCS	Oklahoma Children's Services
OCSE	Office of Child Support Enforcement
OCSS	Oklahoma Child Support Services
OESC	Oklahoma Employment Security Commission
OHCA	Oklahoma Healthcare Authority
OKDHS	Oklahoma Department of Human Services
OMES-ISD	Oklahoma Office of Management and Enterprise Services – Information Services Division
OSDH	Oklahoma State Department of Health
OSF	Oklahoma Office of State Finance
OSIMM	Open Group Service Integration Maturity Model
OSIS	Oklahoma Support Information System
PARB	Post Adjudication Review Board
PHOCIS	Public Health Oklahoma Client Information System
PM	Program Manager

REST	Representational State Transfer
RFP	Request for Proposal
RFQ	Request for Quote
ROI	Return on Investment
SACWIS	Statewide Automated Child Welfare Information System
SAN	Storage Area Network
SDLC	Software Development Life Cycle
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SMI	Structure of Management Information
SNAP	Supplemental Nutrition Assistance Program
SOA	Service Oriented Architecture
SSA	Social Security Administration
SSI	Supplemental Security Income
SSL	Secure Sockets Layer
SSN	Social Security Number
TANF	Temporary Assistance for Needy Families
TOGAF	The Open Group Architecture Framework
UI	User Interface
UIB Data	Utility Integration Bus
VPN	Virtual Private Network
WCF	Windows Communication Foundation
WDML	Wireless Device Markup Language
WIC	Women, Infant and Children
WML	Wireless Markup Language

APPENDIX A – AS-IS SYSTEM INTERFACES

Sender	Interface	Type	Target Agency/Program	Transfer Mechanism	Data Transferred	Frequency Out (In/Out)
KIDS	KIDS Interface - Financial Management Foster Care	External	Finance(AS/400)	FTP	This interface is responsible for paying Foster Care claims through the batch jobs.	Daily, M-F
KIDS	KIDS Interface - Finalist	External		FTP	Address Verification	
KIDS	KIDS Interface - Financial Management Adoptions	External	Finance(AS/400)	FTP	This interface is responsible for paying Forster Care and Adoption claims	1st, Fridays and Last Day of the Month
KIDS	KIDS Interface - Post Payments and Rejects	External	Finance(AS/400)		This interface is responsible for posting payment and claim rejects in KIDS	Daily M-F
KIDS	KIDS Interface - Above Foster Care Authorizations	External	Finance(AS/400)	FTP	This interface is responsible for generating Above Foster Care Authorizations and sending them to Finance	Monthly on the 1st.
Finance (AS/400)	KIDS Interface - Post Above Foster Care Payments	External	KIDS	FTP	This interface is responsible for posting the Above Foster Care Payments made in the prior calendar month in KIDS.	Monthly on the 5th
OHCA	KIDS Interface - Post Medicaid Payments made by OHCA for TFC children	External	KIDS	FTP	Manual process for formatting Excel Spreadsheet and ftp'ing data to WebFOCUS. Then run WebFOCUS job to post payments to KIDS	Monthly when data become available
KIDS	KIDS Interface - Child Care	External	OCCS (Mainframe-IMS)		To process all lines of Day Care Services offered and delivered to the child. It captures service provider information and details regarding the particular service.	
KIDS	KIDS Interface - IV-E	External	AFS		Using the Information comes from PS2 to determine if the child is eligible for the IV-E funding. State pays the foster parents and gets the re-imburement from Feds.	
KIDS	KIDS Interface - DCN	External	AFS (Client Numbering DB(IMS))		DHS client numbering	

90FQ0006 Oklahoma Interoperability Grant Project
 Service-Oriented Architecture (SOA) Roadmap, Revision 2.0 April 26, 2013

Sender	Interface	Type	Target Agency/Program	Transfer Mechanism	Data Transferred	Frequency Out (In/Out)
KIDS	KIDS Interface - AFCARS	External	Federal		Adoption Foster Care Analysis Reporting System	
KIDS	Kids Reporting - FosterCare/Adoption/AFCARS	External	Federal		Foster Care/Adoption/Adoption and Foster Care Analysis and Reporting System (AFCARS)/Ad-hoc Reporting	
KIDS	Kids Reporting - Child Protective Service/NCANDS	External	Federal		Child Protective Service/National Child Abuse and Neglect Data System (NCANDS)/Ad-hoc Reporting	
KIDS	Kids Reporting - Child Protective Service/NYTD	External	Federal		National Youth in Transition Database (NYTD)	
OCSS (Mainframe)	KIDS Interface - CSED	External	KIDS	FTP	The process of receiving data from Child support enforcement Division and update the KIDS DB in order to help workers to determine the IV-E eligibility.	
KIDS	KIDS Interface - Verification Interface jobs completion/Recovery	External	Mainframe(IMS)		The daily interface programs that run to update KIDS or exchange information among different DBs. Verification Interface Jobs Completion/Recovery	
KIDS	G1DX transaction (KIDS IV-E interface with PS2)	External	AFS (PS2)		Reads flat file from KIDS, formats it according to FF trans, and schedules it thru PS2 system. Online trans that lists Data Exchange discrepancies	
KIDS	IV-E and PS2 Interface System	External	AFS (PS3)		Reformats a flat file from KIDS to the FF transaction and schedules it through the PS2 system.	
KIDS	KIDS Interface - Contingency Funds	External	Finance (AS/400)	FTP	List of Cases	Daily M-F
KIDS	KIDS Interface - Targeted Case Management	External	Finance (AS/400)		Provide Finance with a file of Targeted Case Management Claims	Monthly on the last day of the month.
KIDS	KIDS Interface - IV-E Adjustments	External	Finance (AS/400)		Provide Finance with a file of removed children and their current IV-E status and all children where the status changed during the month.	Monthly on the 1st.

90FQ0006 Oklahoma Interoperability Grant Project
 Service-Oriented Architecture (SOA) Roadmap, Revision 2.0 April 26, 2013

Sender	Interface	Type	Target Agency/Program	Transfer Mechanism	Data Transferred	Frequency Out (In/Out)
KIDS	KIDS Interface - New Removals	External	Finance (AS/400)	FTP	Provide Finance with a file in the format of the IV-E adjustments file for children newly removed	Daily
KIDS	Kids PB - Financial Management	External	Finance (AS/400)		This interface is responsible for paying Forster Care and adoptive claims through the batch jobs.	
KIDS	Kids PB - Search/JOLTS/ALFX	External	Mainframe (OJA - Search/JOLTS/ALFX (IMS))		This is a client search process that interfaces to Juvenile On Line Tracking system and DHS Alphabetic Cross Referencing Database.	
OHCA	Citizenship Data	External	AFS		This job copies from OSDH via OHCA/EDS directory for loading Citizenship data to OKDHS mainframe files.	
OESC	New Hire File		AFS		This job reads the State NEW HIRE FILE sent from OESC and adds the data to the State NEW HIRE DATABASE.	
OESC	Wage Data		AFS		This job pulls Wage data file from OESC File Server to OKDHS MAINFRAME	
OESC	UIB File		AFS		This job pulls UIB data file from OESC FILE Server to OKDHS MAINFRAME	
OHCA	Extract File	External	AFS	FTP	THIS JOB FTP'S THE EXTRACT FILE to a FILE on the OKDHS MAINFRAME for OHCA	
OESC	Address File		AFS		This job pulls Monthly ADDRESS file from OESC FILE Server to OKDHS MAINFRAME	Monthly
OESC	Wage File		AFS		This job pulls Monthly WAGE file from OESC FILE Server to OKDHS MAINFRAME	Monthly
OESC	UI File		AFS	FTP	This job FTP OESC monthly UI file to OKDHS mainframe	
OESC	NH Locate Data		AFS	FTP	This job is the FTP to pull the OESC NH locate data from the server to the OKDHS mainframe for transmit to Feds	
OESC	Unemployment File		AFS	TCPFTP	This job gets the UNEMPLOYMENT FILE VIA TCPFTP FROM OESC	

90FQ0006 Oklahoma Interoperability Grant Project
 Service-Oriented Architecture (SOA) Roadmap, Revision 2.0 April 26, 2013

Sender	Interface	Type	Target Agency/Program	Transfer Mechanism	Data Transferred	Frequency Out (In/Out)
AFS	UIB Referral File		OESC		This job will be on request only. It will extract our currently UIB referral file and transfer to OESC.	On Request Only
OESC	OESC Payment File		AFS		This job pulls Weekly a OESC FILE FROM SERVER TO OKDHS MAINFRAME	Weekly
OESC	OESC Address File		AFS		This job pulls a Quarterly OESC ADDRESS FILE from OESC SERVER TO OKDHS MAINFRAME	Quarterly
OESC	OESC Wages File		AFS		This job pulls Quarterly OESC WAGES FILE from OESC SERVER to OKDHS MAINFRAME	Quarterly
OESC	OESC Payment Data		AFS		This job extracts OESC payment data from the OESC server and puts it into a OKDHS mainframe	
AFS	Bendex Data	External	OHCA		This job sends BENDEX DATA TO OHCA/HP	
AFS	Medical Eligibility /O-Epic Roll Data	External	OHCA		This job sends Monthly MEDICAL ELIGIBILITY to MMIS and also sends O-EPIC Monthly ROLL DATA TO MMIS	Monthly
AFS	Medical Eligibility for Recovery	External	OHCA		This is a SPECIAL REQUEST JOB TO SEND MEDICAL ELIGIBILITY TO MMIS for RECOVERY	Special Request
AFS	Medical Eligibility for Recovery	External	OHCA		This is a SPECIAL REQUEST JOB TO SEND MEDICAL ELIGIBILITY TO MMIS for RECOVERY	Special Request
AFS	Third Party Liability	External	OHCA	FTP	This job is the FTP for THIRD PARTY LIABILITY TO OHCA/HP	
AFS	Plan of Care Authorization	External	OHCA	FTP	This job is the FTP PLAN OF CARE AUTHORIZATION TO OHCA/HP	
AFS	Personal Care Authorization	External	OHCA	FTP	This job is the FTP PERSONAL CARE AUTHORIZATION TO OHCA/HP	
AFS	Supportive Living and Non-Fed Medical Authorization	External	OHCA	FTP	This job is the FTP SUPPORTIVE LIVING AND NON-FED MEDICAL AUTHORIZATION TO OHCA/HP	

90FQ0006 Oklahoma Interoperability Grant Project
 Service-Oriented Architecture (SOA) Roadmap, Revision 2.0 April 26, 2013

Sender	Interface	Type	Target Agency/Program	Transfer Mechanism	Data Transferred	Frequency Out (In/Out)
AFS	Citizenship Data	External	OHCA		This job is the Citizenship Data send to OHCA/HP Server (via SFTP) for Oklahoma State Department of Health to pick up the file and execute their process.	
AFS	Eligibility Data	External	OHCA		This job is the Eligibility Data is send to OHCA/HP Server (via SFTP)for Oklahoma Health Care Authority to pick up the file and execute their process.	
AFS	SSN File	External	OESC	FTP	This job creates monthly SSN file to be FTP'd to OESC at month end	Monthly
AFS	NDNH Locate Data		OESC		This job will pull the OESC NDNH Locate data from the OKDHS mainframe to the internal server.	
AFS	UIB Referral File		OESC		This job will create the Weekly UIB REFERRAL FILE that will be transferred to the OESC INTERNET SITE.	Weekly
AFS	Policy Information	External	OHCA		This job downloads POLICY INFORMATION FROM OHCA TO OSIS	
AFS	SVES File	External	OHCA		This job transfers daily SVES file to OHCA/HP from SSA	Daily
AFS	OESC File		OESC		This job sends Weekly OESC FILE TO SERVER FROM MAINFRAME	Weekly
AFS	Mainframe file		OESC		This job puts a MAINFRAME FILE TO FOLDER ON S94X01	
AFS	Mainframe file		OESC		This job puts a MAINFRAME FILE TO FOLDER ON S94X01	
AFS	Absent Parent Data	External	OHCA	SFTP	This job is the Absent Parent Data is send to OHCA/HP Production Server (via SFTP)for Oklahoma Health Care Authority to pick up the file and execute their process.	

90FQ0006 Oklahoma Interoperability Grant Project
 Service-Oriented Architecture (SOA) Roadmap, Revision 2.0 April 26, 2013

Sender	Interface	Type	Target Agency/Program	Transfer Mechanism	Data Transferred	Frequency Out (In/Out)
AFS	Third Party Liability	External	OHCA	SFTP	This job is the Third Party Liability is send to OHCA/HP Production Server (via SFTP) for Oklahoma Health Care Authority to pick up the file and execute their process.	
OHCA	HCPC File	External	AFS		This job is the daily HCPC file from OHCA	Daily
OHCA	HCPC File	External	AFS		This job is the monthly HCPC file from OHCA	Monthly
AFS	SDX File (State Data Exchange)	External	OHCA		This job is the transfer daily SDX file to OHCA/HP	Daily
OCSS	Oklahoma DHS Departmental Client Numbering System	Internal/External	Child Welfare, AFS and OHCA		Allows staff access to Name, SSN and other demographic information regarding OKDHS program participants.	Real Time
OCSS	Oklahoma DHS Departmental Client Numbering System	Internal/External	Child Welfare, AFS, OHCA		Name, SSN and other demographic information about IV-D case participants.	Real Time
OCSS	Oklahoma DHS PS2 Combined Case System	Internal	AFS		Transfer of case participant and eligibility information for TANF and Medicaid Medical Referrals	Real Time
OCSS	Oklahoma DHS PS2 Combined Case System	Internal	AFS		Transfer information regarding TANF benefits issued.	Real Time
OCSS	Oklahoma DHS PS2 Combined Case System	Internal	AFS		OCSS workers manually access PS2 online screens for demographic, benefit and program eligibility information.	Real Time
OCSS	Oklahoma DHS PS2 Combined Case System	Internal	AFS		OCSS sends client cooperation information to AFS	Daily
OCSS	Oklahoma DHS PS2 Combined Case System	Internal	AFS		OCSS sends child support payment information to AFS	Real Time
OCSS	Oklahoma DHS ALFX Cross-reference System	Internal	AFS, CWS		OCSS workers manually search basic demographic information to identify participants in AFS, CWS, OHCA and other OCSS cases.	Real Time
OCSS	Oklahoma DHS ALFX Cross-reference System	Internal	AFS, CWS		OCSS sends Name, SSN and other demographic information for IV-D case participants	Weekly
OCSS	Oklahoma DHS ALFX	Internal	AFS, CWS		OCSS sends Name, SSN and other	Weekly

90FQ0006 Oklahoma Interoperability Grant Project
 Service-Oriented Architecture (SOA) Roadmap, Revision 2.0 April 26, 2013

Sender	Interface	Type	Target Agency/Program	Transfer Mechanism	Data Transferred	Frequency Out (In/Out)
	Cross-reference System				demographic information for SoonerCare case participants	
OCSS	OKDHS KIDS System (child welfare)	Internal	CWS		Transfer NCP demographic, order and financial data (batch files) to the child welfare program regarding Non-IVE Foster Care children.	Monthly
OCSS	OKDHS KIDS System (child welfare)	Internal	CWS		Transfer NCP demographic, order and financial data (batch files) to the child welfare program regarding IV-E Foster Care children.	Monthly
OCSS	Oklahoma DHS PS2 Combined Case System	Internal	CWS		Transfer of case participant and eligibility information for IV-E and non IV-E Foster Care Referrals	Real Time
OCSS	OKDHS Finance System	Internal	CWS		OKDHS finance sends records of IV-E benefits expended for input to the OCSS URA process.	Monthly
OCSS	OKDHS Finance System	Internal	CWS		OCSS workers manually query IV-E benefits expended on the Finance AS400 system.	Real Time
OCSS	TPL (Third Party Liability) Interface	External	OHCA		OCSS Receive Insurance coverage information	Weekly
OCSS	TPL (Third Party Liability) Interface	External	OHCA		OCSS Receive Insurance and Carrier information	Daily
OCSS	Oklahoma Health Care Authority	External	OHCA		Send IV-D case participant demographic and CP cooperation information updates to OHCA	Daily
OCSS	Oklahoma Health Care Authority	External	OHCA		Transfer of case participant and eligibility information for Medical Referrals.	Daily
OCSS	Online Enrollment	External	OHCA		OCSS reviews case participant and eligibility information for SoonerCare cases.	Real Time
OCSS	MMIS	External	OHCA		OCSS reviews case participant and eligibility information for SoonerCare cases.	Real time
OCSS	SSA	External	Other State IV-D programs		Connections through CSENet receiving IVA, IVE and XIX eligibility for IV-D case participants.	Daily
OCSS	SSA	External	Other State IV-D programs		Connections through State Services Portal (SSP) receiving IVA, IVE and XIX eligibility for IV-D case participants.	Real Time
OCSS	SSA	External	Other State IV-D		Connections through CSENet sending IVA, IVE	Daily

90FQ0006 Oklahoma Interoperability Grant Project
 Service-Oriented Architecture (SOA) Roadmap, Revision 2.0 April 26, 2013

Sender	Interface	Type	Target Agency/Program	Transfer Mechanism	Data Transferred	Frequency Out (In/Out)
			programs		and XIX eligibility for IV-D case participants.	
OCSS	SSA	External	Other State IV-D programs		Connections through State Services Portal (SSP) sending IVA, IVE and XIX eligibility for IV-D case participants.	Real Time
OCSS	TPL (Third Party Liability) Interface	Internal	AFS		OCSS sends updated insurance policy information to AFS.	Weekly
OSDH	Birth Data	External	OCSS		This interface transfers Vital Records e.g. Birth Data	
OHCA	FP Recipient with TPL Extract	External	OSDH		Extract that has MMIS recipient that are eligible for FP that have other insurance	Once a Month. 1st day of the month
OHCA	BCC recipients with TPL extract	External	OSDH		Extract that has MMIS recipient that are eligible for BCC that have other insurance	Once a Month. 1st day of the month
OHCA	Daily Application Batch File	External	OSDH		Daily extract of applications submitted or updated the previous day	Daily
OHCA	OSDH Citizenship Request File	External	OSDH		Daily extract of citizenship requests	Daily
OSDH	OSDH Citizenship Response File	External	OHCA		Daily extract of citizenship responses	Daily
AFS	Prior Authorizations Update	External	OHCA		Advantage Waiver Prior Authorizations	Daily Mon-Fri
OHCA	Prior Authorizations Update	External	AFS		PS2 Personal Care PA Update Report	Daily Mon-Fri
OHCA	Prior Authorizations Update	External	AFS		PS2 Personal Care PA Update Error Report	Daily Mon-Fri
OHCA	Prior Authorizations Update	External	AFS		Advantage Waiver Update Report	Daily Mon-Fri
OHCA	Prior Authorizations Update	External	AFS		Advantage Waiver Update Error Report	Daily Mon-Fri

APPENDIX B – AS-IS AGENCY PROGRAMS

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

90FQ0006 Oklahoma Interoperability Grant Project
 Service-Oriented Architecture (SOA) Roadmap, Revision 2.0 April 26, 2013

KDHS – 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 (Public Health Oklahoma 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

90FQ0006 Oklahoma Interoperability Grant Project
 Service-Oriented Architecture (SOA) Roadmap, Revision 2.0 April 26, 2013

	OHCA - Online Enrollment	Agency Partner - OSHD 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><i>* Oklahoma will not have an exchange of its own. OHCA will coordinate with the Federal exchange but not have any control over it. 1 OHCA will intake info and if the applicant is not eligible for Medicaid info will be sent to the exchange. Details unknown at this time.</i></p>								

APPENDIX C – AS-IS SYSTEM OVERVIEW

1 AS-IS SYSTEM OVERVIEW

Figure C-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))

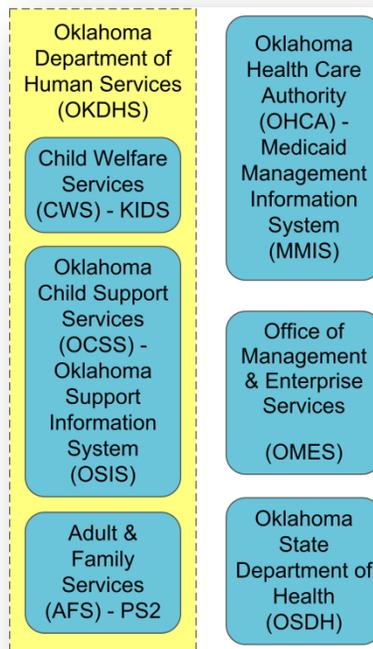


Figure C-1: AS-IS System Overview

The systems/owners identified in the Interoperability Project are shown in Table C-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 C-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)

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

1.1 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 C-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.

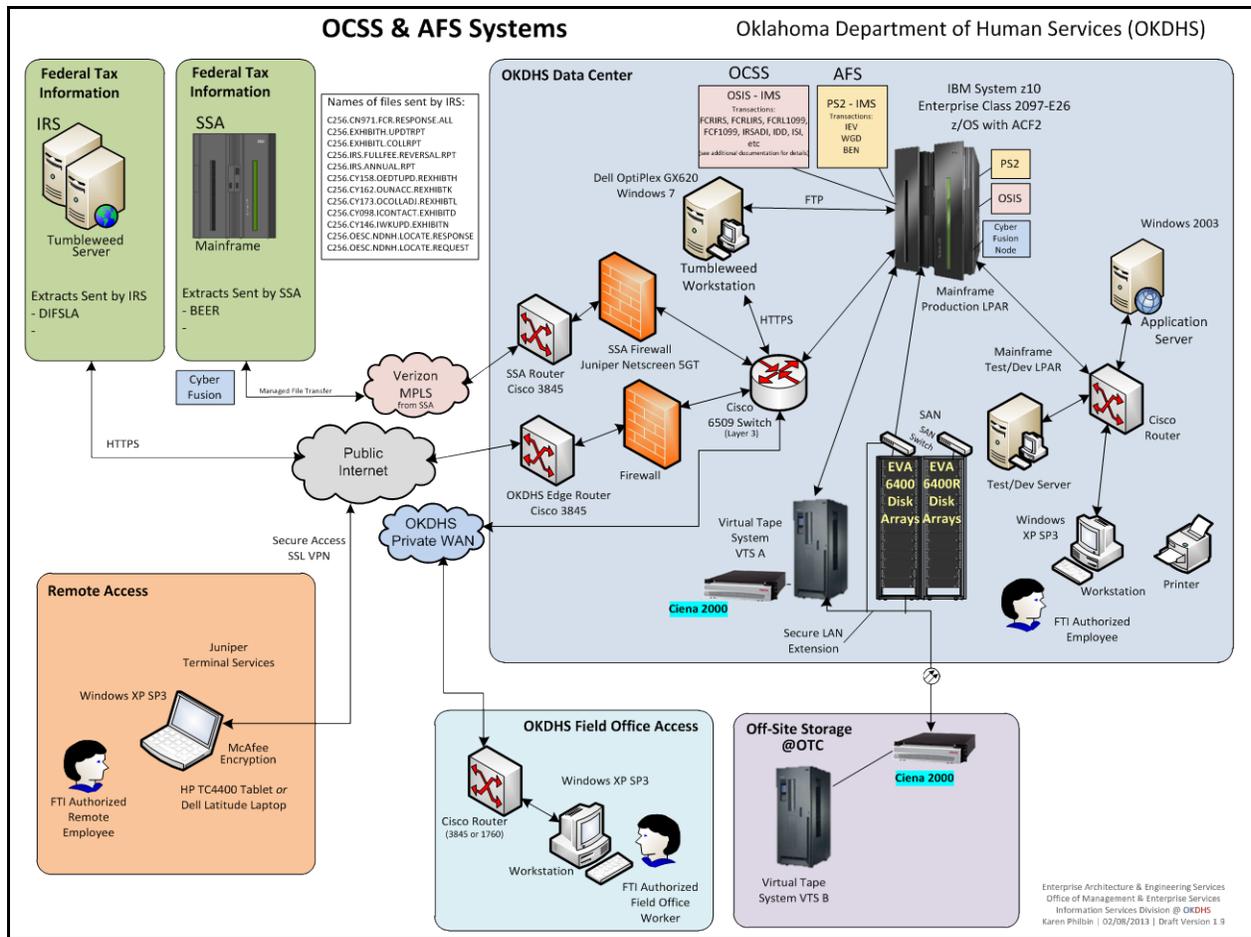


Figure C-3: Overview of OCSS and AFS Systems

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

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.

1.2.1 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 C-5 illustrates the AS-IS Eligibility and Enrollment data exchanges for AFS.

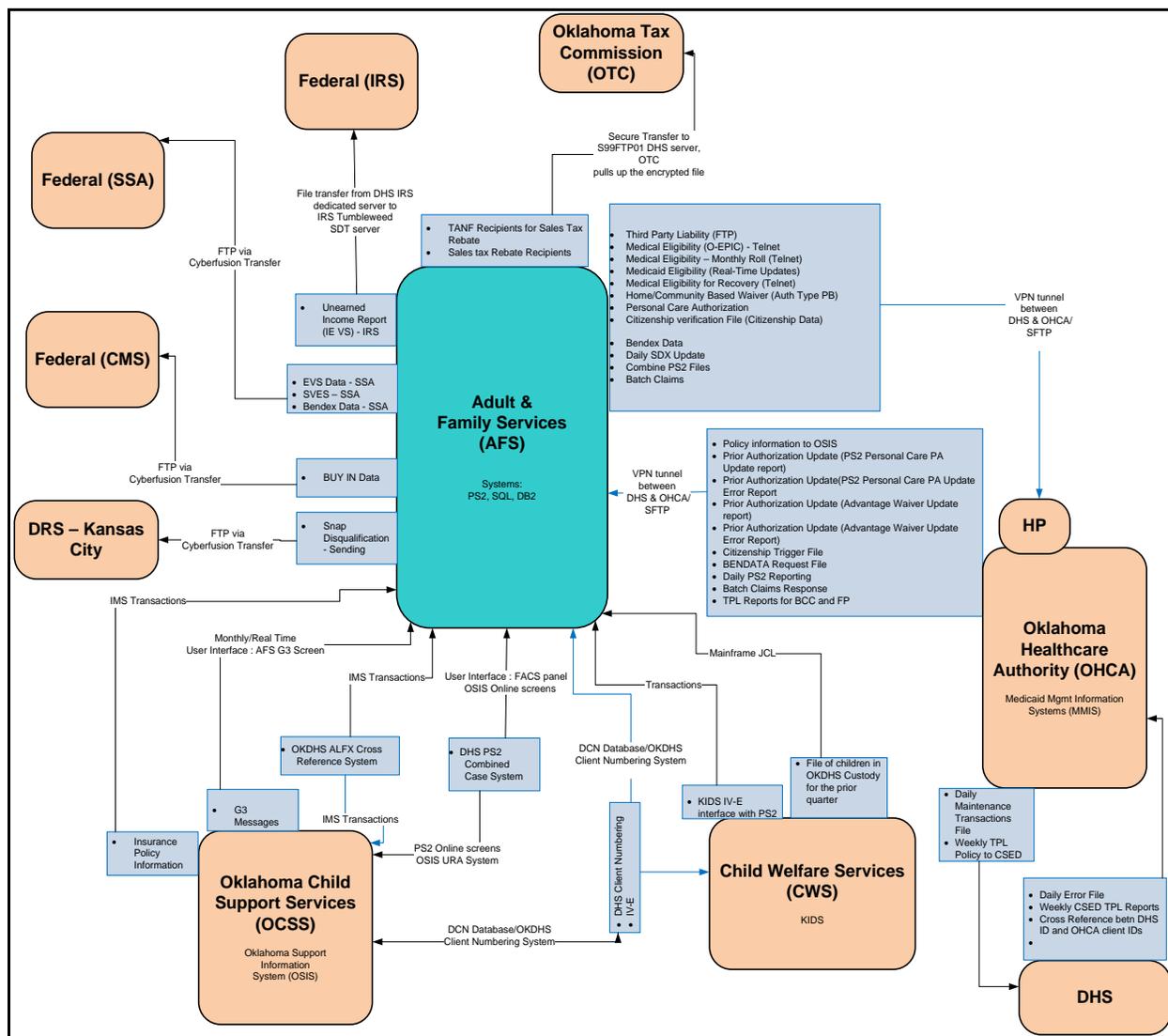


Figure C-5: AS-IS Eligibility and Enrollment Interfaces for AFS

1.3 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 C-6 provides a high level overview of the KIDS Application Architecture.

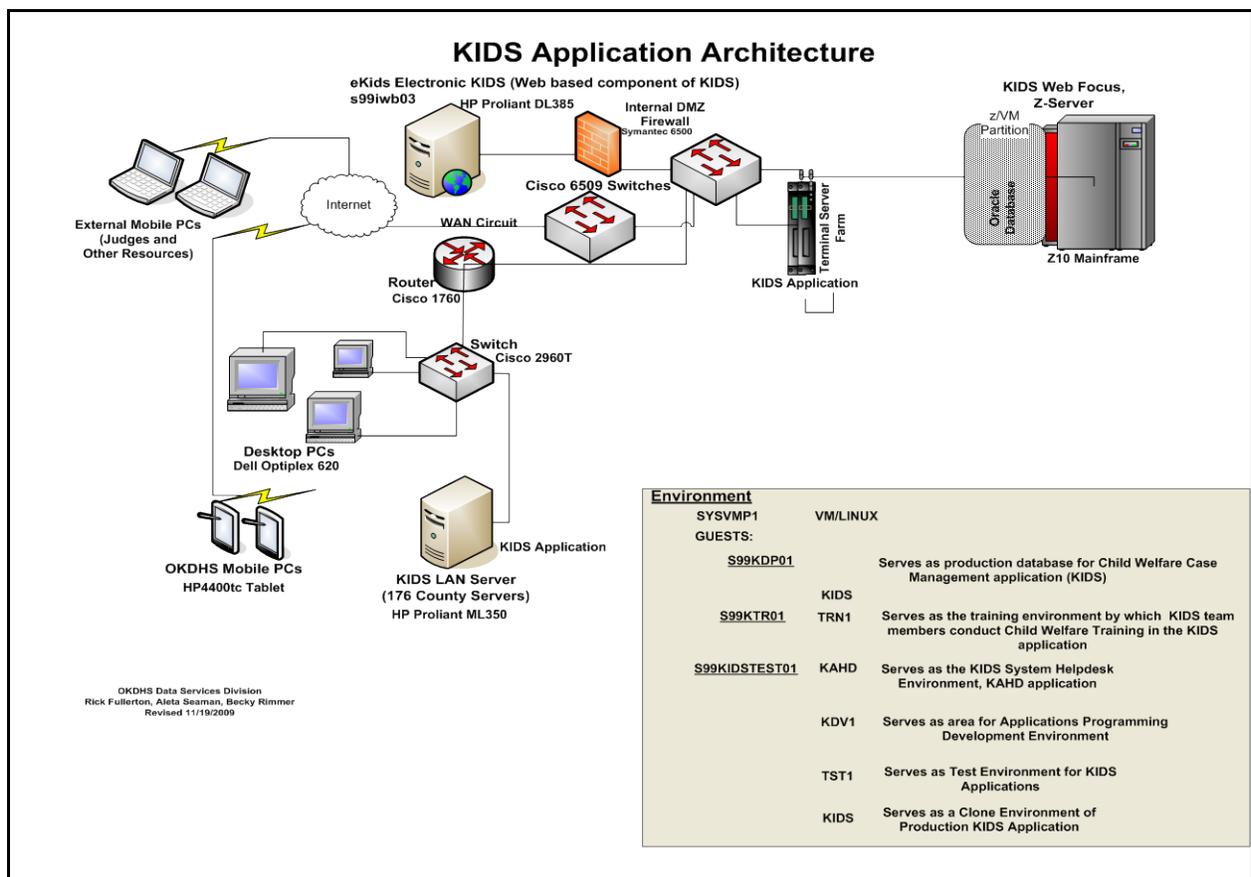


Figure C-6: KIDS Application Architecture

Figure C-7 illustrates a functional view for KIDS

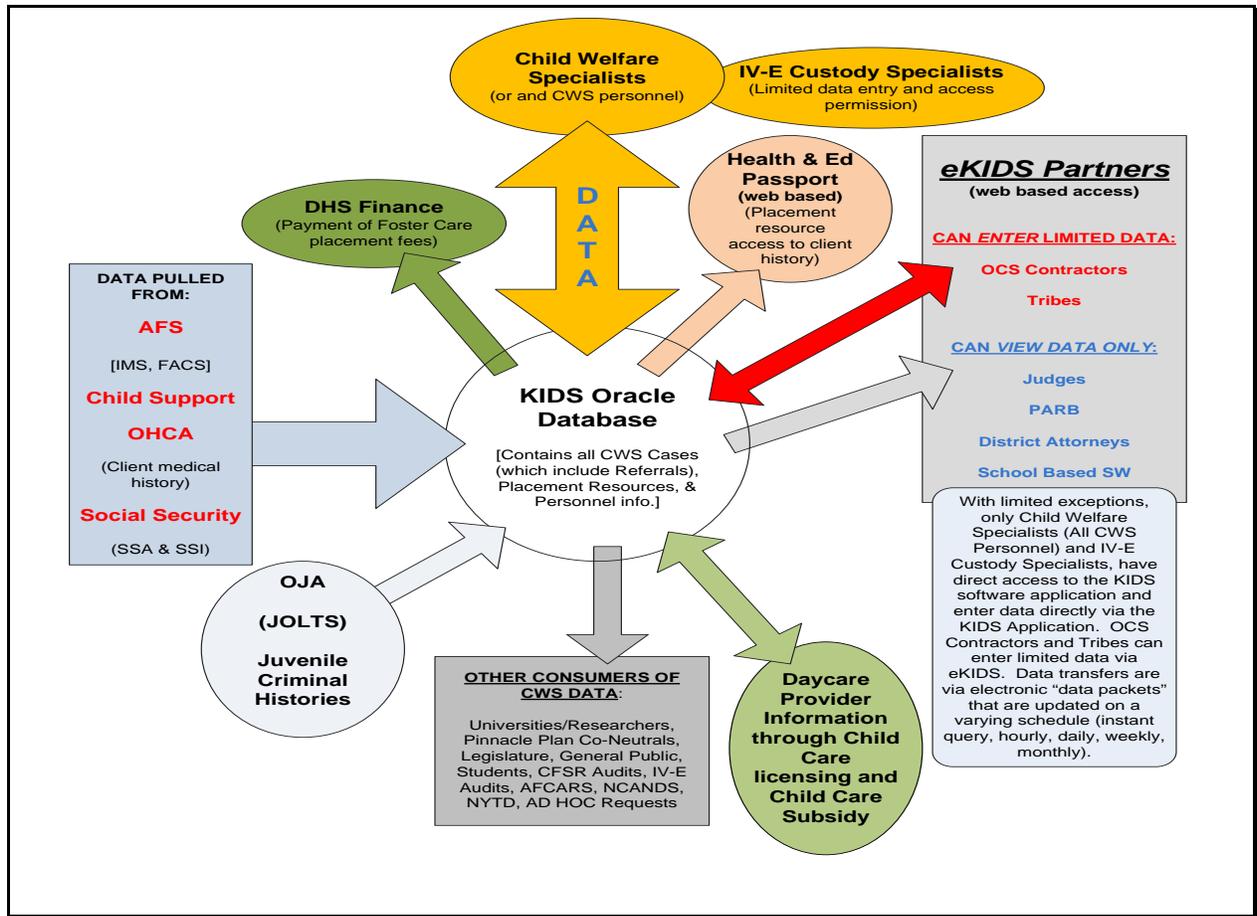


Figure C-7: KIDS System

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 C-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.

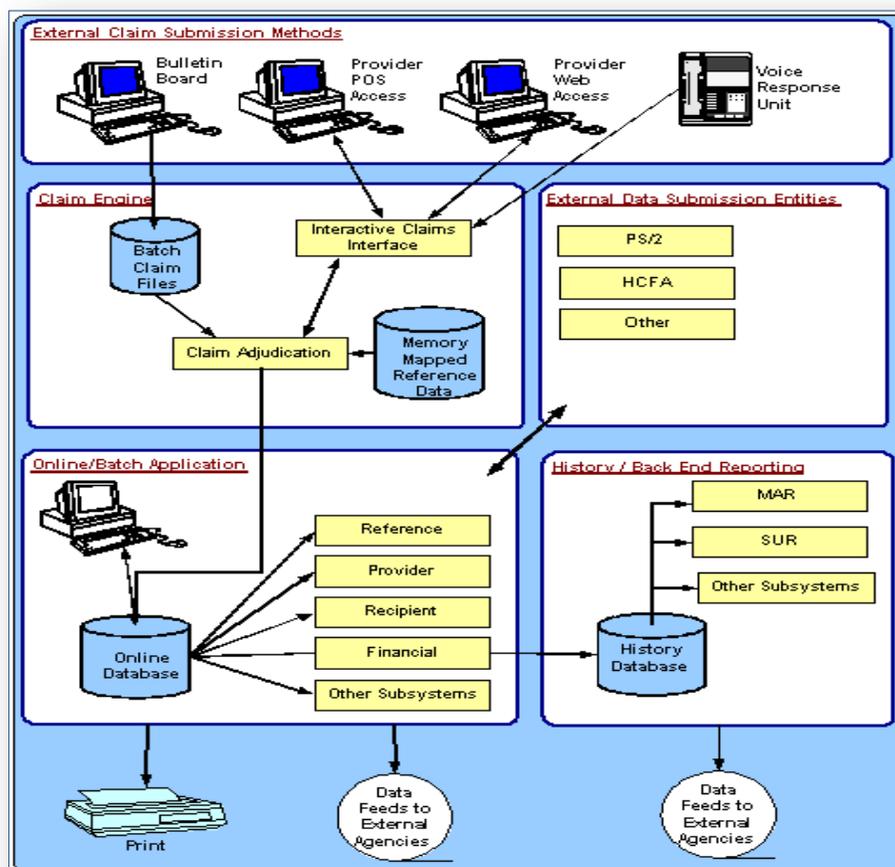


Figure C-9: MMIS Logical Components

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

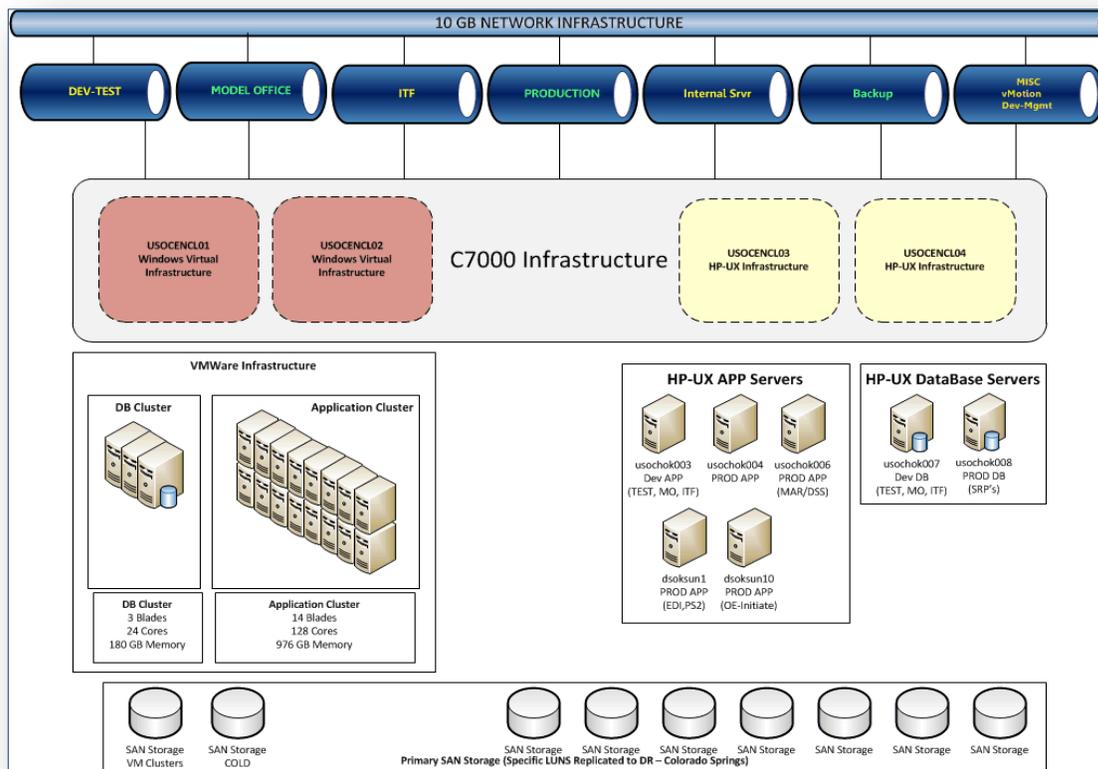


Figure C-10: MMIS Architecture

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

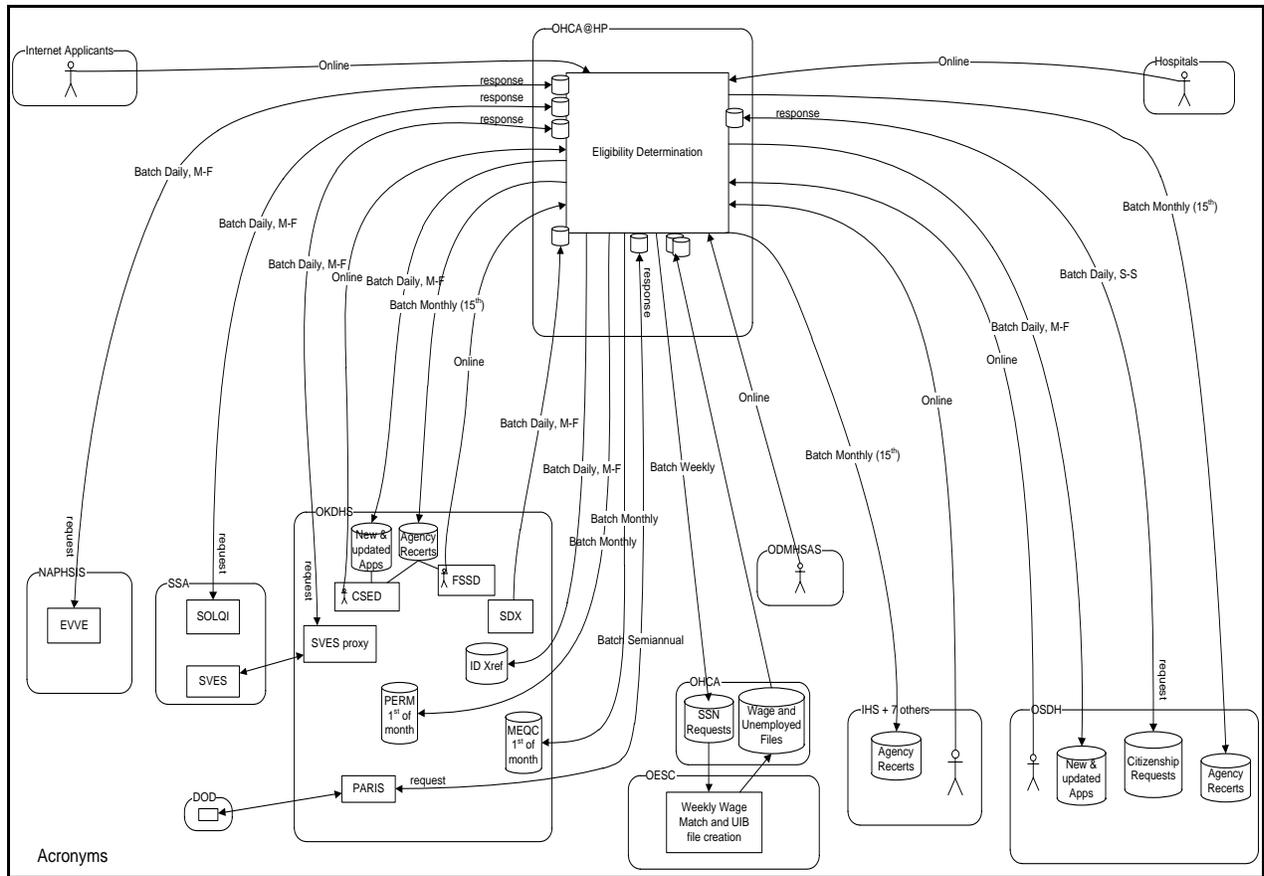


Figure C-11: AS-IS Eligibility Determination Functional View for OHCA

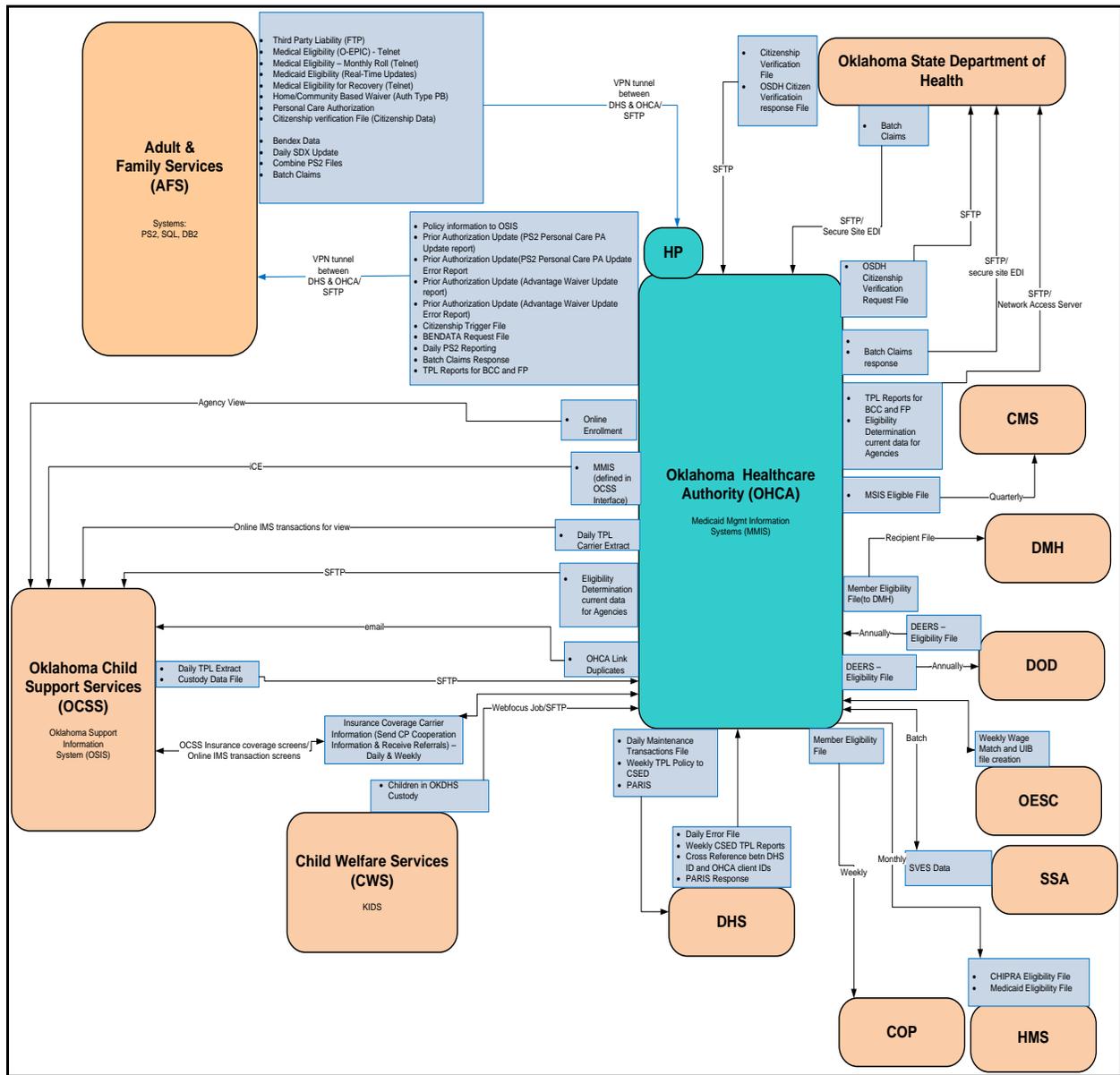


Figure C-12: AS-IS Eligibility and Enrollment Interfaces for OHCA

1.5 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 C-13 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 a 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.

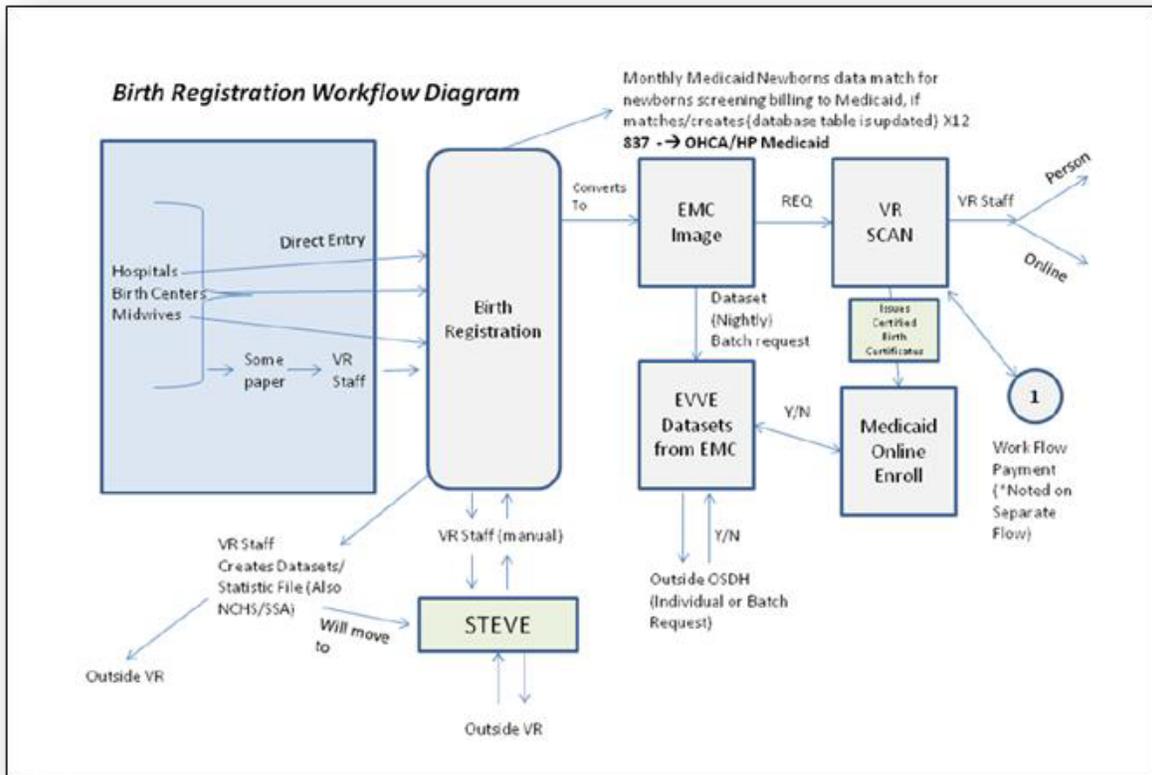


Figure C-13: OSDH – Vital Records, Birth Registration Workflow

1.5.1 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.

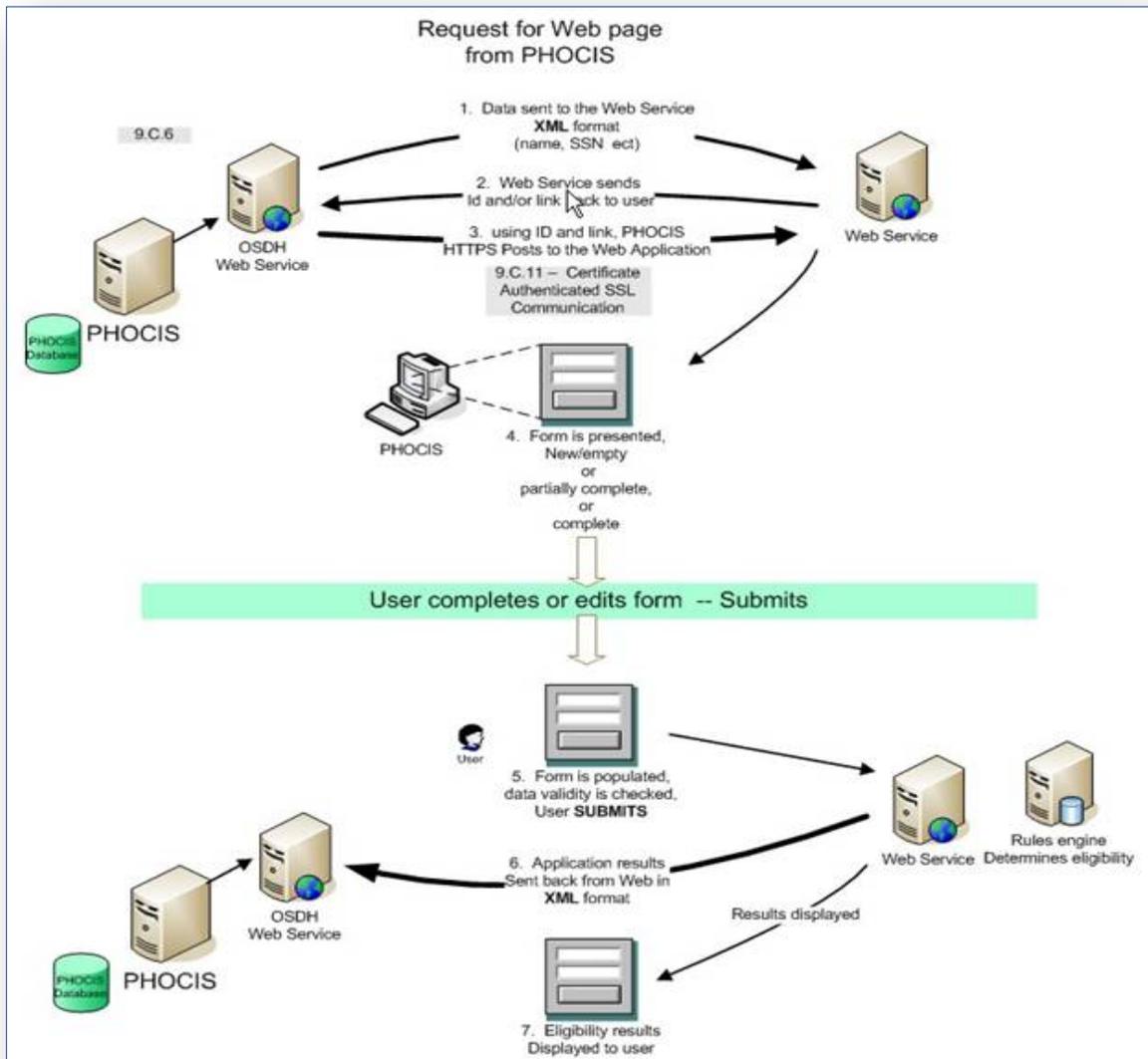


Figure C-14: PHOCIS

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

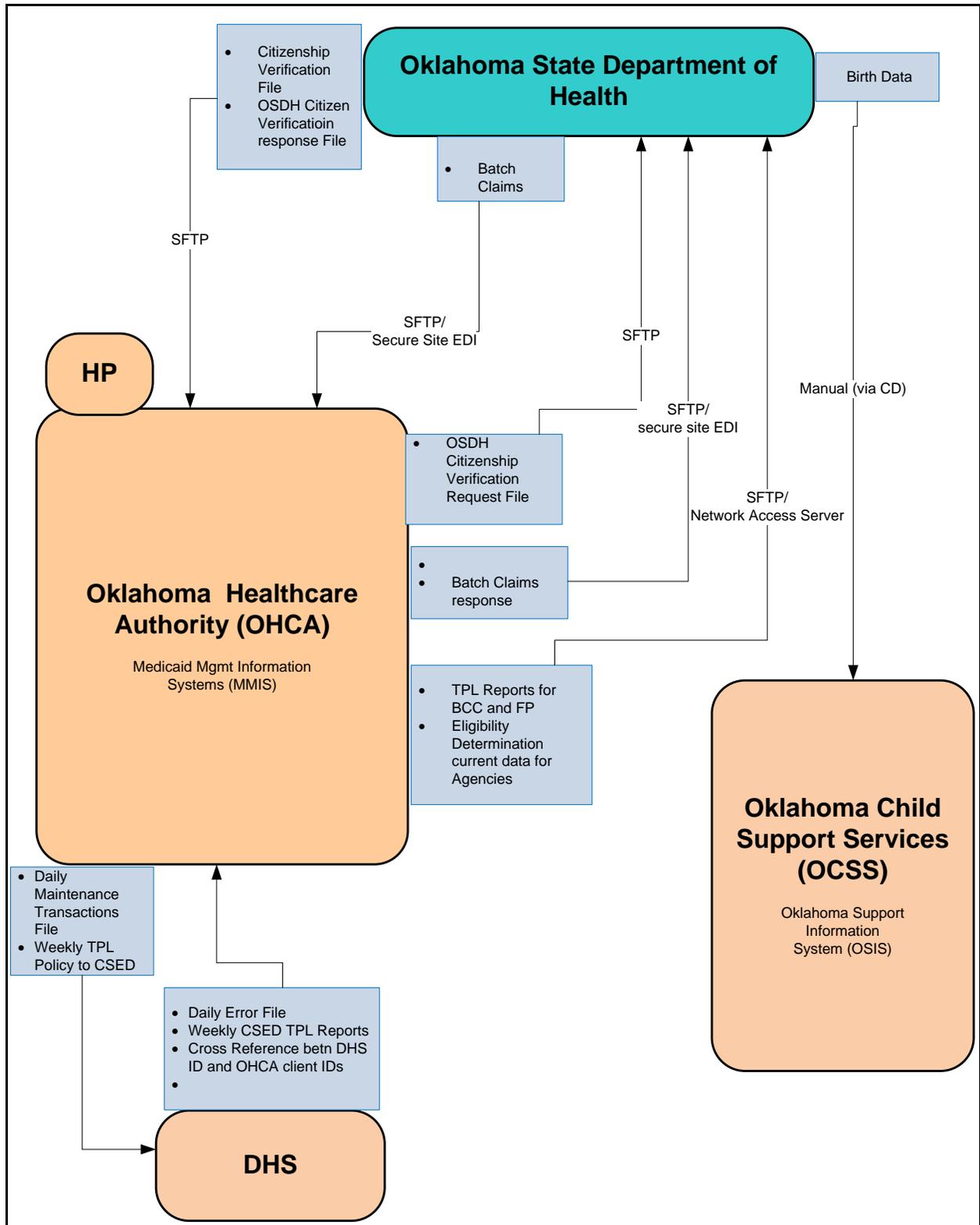


Figure C-15: Eligibility and Enrollment Interfaces for OSDH

2 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.

2.1 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

2.2 Clients

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

- OSIS via IVR
- Web Portal
- CARE Call Center

2.3 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.

2.4 Other States

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

2.5 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

2.6 Management

The same access as Case Workers to the various interfaces.

2.7 Reporting Module

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

- WebFOCUS
- RDS/Document Direct

2.8 Oklahoma Public Health Module

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

2.9 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

2.10 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

2.11 Adult and Family Services (AFS) Module

AFS exchanges data (interfaces) with OCSS and OHCA.

2.12 Oklahoma Child Support Services (OCSS) Module

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

2.13 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.

2.14 Oklahoma Providers Module

2.14.1 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.

2.14.2 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.