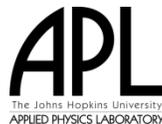


Prepared for the:
Administration for Children and Families (ACF)

National Human Services Interoperability Architecture
Project Viewpoint Description
DRAFT Version D0.3
September 2012

Prepared by:
The Johns Hopkins University
Applied Physics Laboratory (JHU/APL)



Draft Issue

It is important to note that this is a draft document. The document is incomplete and may contain sections that have not been completely reviewed internally. The material presented herein will undergo several iterations of review and comment before a baseline version is published.

This document is disseminated in the interest of information exchange. The Johns Hopkins University Applied Physics Laboratory (JHU/APL) assumes no liability for its contents or use thereof. This report does not constitute a standard, specification, or regulation. JHU/APL does not endorse products or manufacturers. Trade and manufacturer's names appear in this report only because they are considered essential to the object of this document.

Note: This document and other NHSIA-related documents are available for review from the Administration for Children and Families (ACF) Interoperability Initiative website. The URL for the site is currently: <http://transition.acf.hhs.gov/initiatives-priorities/interoperability>. When ACF completes the migration to their new website the URL is expected to be <http://www.acf.hhs.gov/initiatives-priorities/interoperability>.

Review and comments to this document are welcome. To comment, please contact Joseph Bodmer at joseph.bodmer@acf.hhs.gov or 202-690-1234.

Valerie B. Barnes
The Johns Hopkins University Applied Physics Laboratory
11100 Johns Hopkins Road
Laurel, MD 20723
Phone: 717-352-0131
E-Mail: Valerie.Barnes@jhuapl.edu

Table 1. Revision History

Version	Date	Description of Change	Reference	Edited Location	Executor
D0.3	2012-09	Original version published. This document merges and reworks three artifacts from the D0.2 Project Viewpoint: Implementation Strategy, Jurisdiction's Guide to NHSIA Implementation, and Federal Program's Guide to NHSIA Implementation			VBB

This page intentionally blank

Table of Contents

1	Introduction	1
1.1	NHSIA Overview and Objectives.....	1
1.2	Architecture Framework and Viewpoints	1
1.3	Architecture Documentation.....	2
2	Project Viewpoint Summary	5
2.1	Project Viewpoint Description	5
2.2	Project Viewpoint Artifacts	5
3	Overview of Implementation Approach for Jurisdictions	7
3.1	State Diversity and Commonality	7
3.2	NHSIA Core	10
3.3	NHSIA System of Systems.....	12
3.4	Roadmap	13
3.5	Jurisdiction's Steps.....	14
4	Assess Current Situation	17
5	Plan and Design.....	19
6	Support NIEM Standards Development.....	21
7	Prototype or Pilot Parts of NHSIA.....	23
7.1	Establish the Infrastructure	24
7.2	Establish Core IT Services	24
7.3	Establish a County and/or State Hub.....	25
7.4	Establish End-User Capability	26
8	Update Plan and Design; Implement NHSIA Incrementally	29
8.1	Update NHSIA Plan and Design	29
8.2	Implement NHSIA Incrementally	30
8.2.1	Elements to Support Core Capabilities	31
8.2.2	Common Elements	41
8.2.3	Custom Elements	42
8.3	Share with Other Jurisdictions	42
9	Recap	43
10	References	45
	Appendix A – Accessibility Appendix	47
	Appendix B – Global Reference Architecture Documents.....	49

List of Figures

Figure 1-1. NHSIA Viewpoints	2
Figure 1-2. NHSIA Viewpoints with Artifacts	3
Figure 2-1. The Project Viewpoint Reflects Key Elements from Other Viewpoints ...	6
Figure 3-1. States Have Different Models for Organizing and Supporting Human Services	8
Figure 3-2. NHSIA Core Supports All Business Areas	11
Figure 3-3. Notional NHSIA Roadmap	14
Figure 3-4. Jurisdiction's Steps to Implement NHSIA	15
Figure 7-1. Example County Pilot Deployment of NHSIA	27
Figure 8-1. Iterative Process for Incremental Implementation.....	29
Figure 8-2. Notional IT Environment for a County that Adopts NHSIA.....	32
Figure 8-3. Notional Access Control	37
Figure 8-4. Reference Model: Performance Information Repositories	39
Figure 8-5. A Catalog Is One Way to Make Information about Hubs Available	41
Figure 9-1. Jurisdiction's Steps to Implement NHSIA (repeated)	43
Figure 9-2. Iterative Process for Incremental Deployment (repeated).....	44

List of Tables

Table 1. Revision History	i
Table 2. Project Viewpoint Artifacts	6
Table 3. Notional Common Client Authorization "Form"	36
Table 4. GRA Documents	51

1 Introduction

1.1 NHSIA Overview and Objectives

The National Human Services Interoperability Architecture is being developed by the Administration for Children and Families (ACF) as a framework to support integrated eligibility determination and information sharing across programs and agencies, improved delivery of services, prevention of fraud, and better outcomes for children and families. It consists of business, information, and technology models to guide programs and states in improving human service administration and delivery through improved interoperability of business processes and information technology (IT).

The primary goal of the NHSIA Project is to develop a national architecture to enable information exchange and sharing IT services across currently siloed federal, state, local, and private human service information systems. It is envisioned that the ultimate outcome for stakeholders following NHSIA guidance will be:

- Interoperability of IT elements and associated business processes
- Improved care provided to clients by holistically addressing their needs - e.g., "no wrong door"
- Comprehensive, integrated support for client-oriented case workers at point of service
- Incremental insertion of new services and technology
- More flexible, adaptive systems
- Reduced cost of operation and maintenance through sharing and reuse of services, data, and IT resources
- Reduced fraud through automated and coordinated enrollment, verification and eligibility determination
- Greater availability of timely program data for evaluating program performance
- Better connections between human services and health and education services, and the ability to leverage advances made in those areas

1.2 Architecture Framework and Viewpoints

An **architecture** is a description of the components, structure, and unifying characteristics of a system. An enterprise architecture is a rigorous, comprehensive description of an enterprise, including mission and goals; organizational structures, functions, and processes; and information technology including software, hardware, networks, and external interfaces. NHSIA can be thought of as a multi-enterprise, or **community architecture**.

An **architectural framework** is a structure for describing an architecture. The NHSIA project has adapted the frameworks defined by the Federal Enterprise Architecture (FEA)¹ and the DoD Architectural Framework (DoDAF)², and has incorporated applicable features of the Medicaid IT Architecture (MITA) Framework³. DODAF has evolved over a decade to include multiple viewpoints. NHSIA has adapted DODAF to include the viewpoints shown in Figure 1-1. 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.

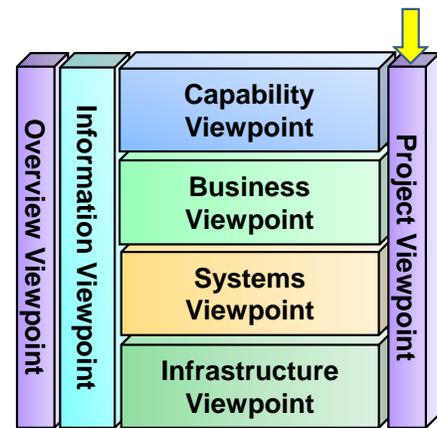


Figure 1-1. NHSIA Viewpoints

1.3 Architecture Documentation

NHSIA is documented by a viewpoint description for each viewpoint. Each of these viewpoint descriptions is supported by more detailed documents including white papers, spreadsheets, diagrams, presentations, and products of specialized architectural tools. The viewpoint descriptions and associated products are referred to as architectural artifacts. This viewpoint description document addresses the Project Viewpoint.

This is the first version of the Project Viewpoint Description; it is labeled as D0.3 because it is part of the third major set of draft NHSIA documents. This document merges and reworks three artifacts delivered as part of the D0.2 Project Viewpoint. This document replaces these three D0.2 artifacts: NHSIA Implementation Strategy, the Jurisdiction's Guide to NHSIA Implementation, and the Federal Program's Guide to NHSIA Implementation.

This document describes an approach and projects a jurisdiction should consider to implement NHSIA. This document refers to the artifacts published for NHSIA; they are organized according to viewpoint. Figure 1-2 illustrates the viewpoints and artifacts. See the Overview Viewpoint for more background about the NHSIA project and each viewpoint.

¹ <http://www.whitehouse.gov/omb/e-gov/fea/>

² DoD Architecture Framework, version 2.0, Volume 1: Introduction, Overview and Concepts, Manager's Guide, 28 May 2009.

³ <https://www.cms.gov/MedicaidInfoTechArch/>

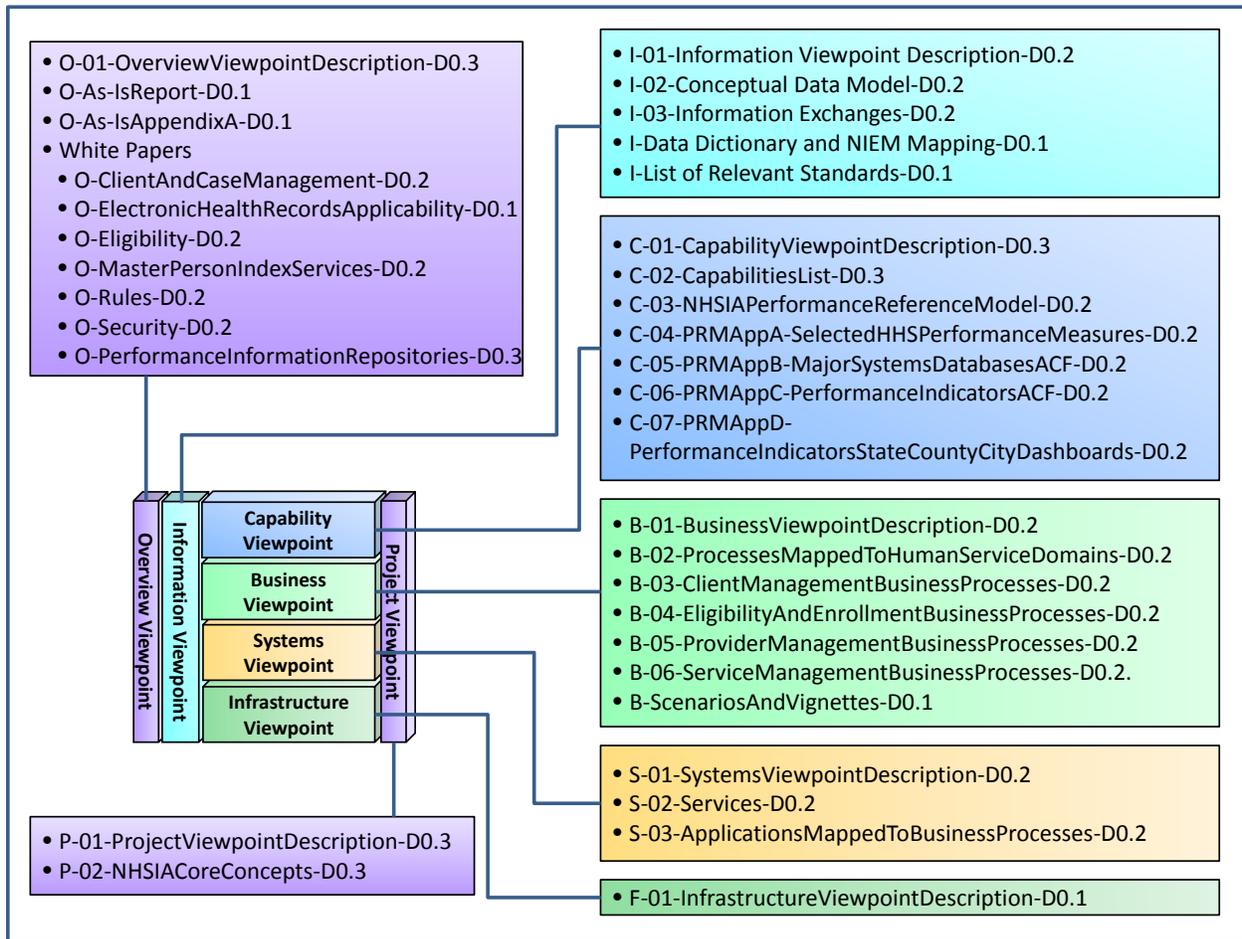


Figure 1-2. NHSIA Viewpoints with Artifacts

The reader is advised that some material appears in both of the Project Viewpoint artifacts. This lets each document stand alone.

This page intentionally blank

2 Project Viewpoint Summary

The Project Viewpoint proposes an approach that a jurisdiction may consider to implement the capabilities defined by the NHSIA architecture. It outlines how the transition from the as-is human services information systems architecture to the desired to-be architecture might be made. The primary audience is the members of the human services community at the state or county level of government who are responsible for developing strategic plans, projects, and budgets to effect the transition.

In the context of NHSIA implementation, we use the term “jurisdiction” to mean the region or geo-political unit that is responsible for the management and/or administration of human services. A “jurisdiction” may be a state, one or more counties, or one or more municipalities - depending on how the management and administration of human services are organized. The agencies, staff members, and other stakeholders in a jurisdiction will collaborate to implement NHSIA.

While the main audience for this viewpoint is staff from state and local jurisdictions, some aspects of the viewpoint may also be applicable to federal programs. In particular, federal program staff may evaluate which NHSIA concepts should be adopted to support outward-facing operations (i.e., the operations that involve interacting with citizens, jurisdictions, and providers).

2.1 Project Viewpoint Description

This document describes a multi-step, multi-year approach for implementing NHSIA. Each jurisdiction starts at a different point in terms of which NHSIA capabilities are already in place; how human services activities and information are organized and managed; priorities for improvements; and resources to effect change. The implementation approach described here is intended to be general enough to apply to most situations, yet specific enough to guide the process of moving from the as-is architecture to a desired to-be end state.

2.2 Project Viewpoint Artifacts

Table 2 summarizes the major artifacts currently included in the Project Viewpoint.

Table 2. Project Viewpoint Artifacts

Artifact	Form & Description
Project Viewpoint Description: Implementation Approach	Form: The remainder of this document. A narrative document including text and figures.
	Description: An approach for the transition from the as-is situation to the NHSIA to-be architecture. To be used primarily by the members of the human services community at the state and local levels of government who are responsible for developing strategic plans, programs, and budgets to effect the transition.
“NHSIA Core” Concepts	Form: A narrative document including text and figures.
	Description: Definition of NHSIA core capabilities, related concepts, and implementation building on those concepts.

As shown in Figure 2-1, the Project Viewpoint builds on elements from the other basic viewpoints.

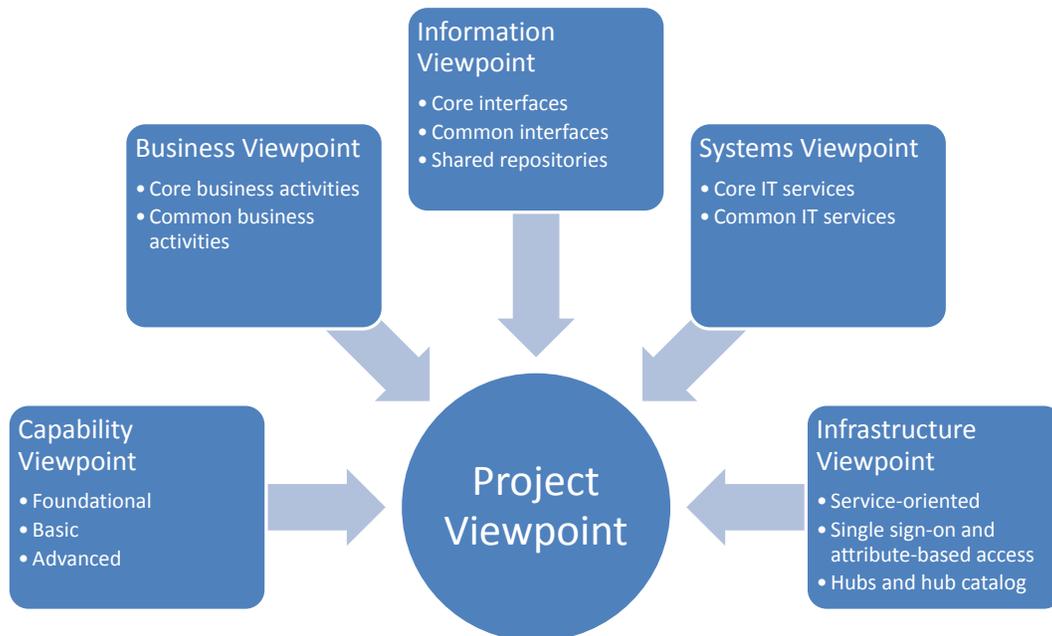


Figure 2-1. The Project Viewpoint Reflects Key Elements from Other Viewpoints

3 Overview of Implementation Approach for Jurisdictions

The implementation strategy is to leverage the development of reusable IT components (e.g., IT services, information exchanges, and information repositories). The IT services may be built once and invoked by many applications, or built as a model for others to use in their own implementation. New information exchanges should use standards, primarily based on the National Information Exchange Model (NIEM) vocabulary. The information repositories may be virtual or actual.

Remaining sections in this chapter describe key elements of the implementation strategy.

3.1 State Diversity and Commonality

Each state has its own approach for organizing, managing, administering, delivering, and supporting human services. For instance, in Maryland, the state's Department of Human Resources supervises and administers most human services programs with staff members placed in each county. One exception is Montgomery County, MD, where the Montgomery County Department of Health and Human Services administers most human services programs. In New York, multiple state-level departments supervise the range of human services; counties administer most human services programs. There may be many information technology (IT) environments in a single state. For instance, there may be an IT environment used by human services staff members at the state level and separate IT environments used in each county to support human services. In some cases, the same software application may be used across the state for one human services program; in others, a different software application may support the same function in each county. Components of the IT infrastructure (e.g., network, database servers, application servers) may be shared across the county, may support one county department or agency, may support all human services staff members in the state, and many variations in between. Figure 3-1 illustrates some of the dimensions that may vary between jurisdictions and across human services programs.

The National Human Services Interoperability Architecture applies to any state model. The architecture addresses information systems that provide capabilities to support the business activities associated with the management, administration, and/or delivery of human services. NHSIA focuses on enabling information exchange and sharing IT services among information systems, whether those systems are managed and/or operated by state, local/tribal, or private organizations.

Undertaking NHSIA implementation is likely to be an effort that involves representatives from several agencies or program offices within the state. If the human services are administered at the local level, then local representatives will

also be involved. For simplicity, we will call those involved with implementing NHSIA in a jurisdiction the “Jurisdiction NHSIA Team”. The Jurisdiction NHSIA Team should address all the IT environments used to support human services.

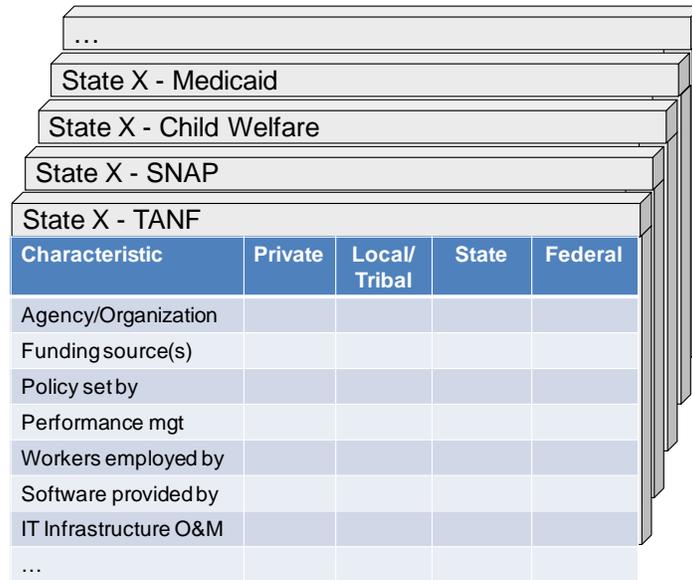


Figure 3-1. States Have Different Models for Organizing and Supporting Human Services

Each jurisdiction that is undertaking NHSIA may want to establish a NHSIA program management office to manage the effort. If the jurisdiction has 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.

The importance of effective governance cannot be overemphasized as stated in the Open Group guidance on Elements of an Effective Architecture Governance Strategy⁴:

An enterprise architecture imposed without appropriate political backing is bound to fail. In order to succeed, the enterprise architecture must reflect the needs of the organization. Enterprise architects, if they are not involved in the development of business strategy, must at least have a fundamental understanding of it and of the prevailing business issues facing the organization. It may even be necessary for them to be involved in the system deployment process and to ultimately own the investment and product selection decisions arising from the implementation of the Technology Architecture.

There are three important elements of architecture governance strategy that relate particularly to the acceptance and success of architecture within the enterprise. While relevant and applicable in their own right apart from their role in governance, and therefore described separately, they also form an integral part of any effective architecture governance strategy. A cross-organizational Architecture Board must be established with the backing of top management to oversee the

⁴ The Open Group Architecture Framework (TOGAF) Version 9.1, the Open Group, <https://www2.opengroup.org/ogsys/jsp/publications/mainPage.jsp>, Chapter 50, 2009.

implementation of the IT governance strategy. A comprehensive set of architecture principles should be established, to guide, inform, and support the way in which an organization sets about fulfilling its mission through the use of IT. An Architecture Compliance strategy should be adopted — specific measures (more than just a statement of policy) to ensure compliance with the architecture, including Project Impact Assessments, a formal Architecture Compliance review process, and possibly including the involvement of the architecture team in product procurement.

3.2 NHSIA Core

NHSIA is likely to be implemented via an evolutionary approach. The approach that NHSIA is taking is to architect a core⁵ 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.** Defining a core provides a clear target for initial implementation. Decision-makers should consider the core capabilities when funding and prioritizing projects and when ordering the sequence of implementation activities. The list of core elements provides a yardstick to measure progress in implementing NHSIA.

The **core NHSIA capabilities**:

- Provide a foundation for interoperability (among programs, agencies/organizations, and jurisdictions). Interoperable systems share information and IT services to efficiently deliver integrated human services to the client community. Interoperability can be achieved via the design and implementation of systems compatible with NHSIA, which defines the principles, standards, IT services, security measures, and interfaces to be followed by the component elements within the total system of systems⁶.
- Provide foundational capabilities or information.
 - Find and get basic and/or summary information about key entities (person, case, provider, and program) to improve information sharing and enable improved delivery of human services
 - Verify information against authoritative sources to support eligibility and other program-related rules

⁵ See the "NHSIA Core" Concepts, Draft version D0.3, September 2012.

⁶ Note that the initial versions of NHSIA do not define all the standards, IT services, etc. necessary to completely achieve the capabilities. The initial versions of NHSIA focused on a subset of the span of human services business processes.

- Collect, aggregate, and analyze key operational performance information across programs and agencies/organizations to improve effectiveness and efficiency

As one example of interoperability, the core foundation should provide user identity management to allow information system users to access the tools and information they need across multiple systems via a single set of credentials. This is sometimes called “single sign-on”. Another foundational element is the Master Person Index (MPI) which enables matching records about people.

Figure 3-2 illustrates that the NHSIA core supports all the business areas involved in human services. Initial work on NHSIA addressed the green business areas in some detail; yellow areas were defined at a high level. The core elements provide functionality upon which end-user capabilities can be built. To realize value of the core capabilities, an agency/organization should implement the core capabilities and implement or adapt one or more high-priority end-user business capabilities building on the core elements. The implementation would likely invoke core, other common, and custom IT services. Figure 3-2 identifies a few candidate end-user capabilities.⁷

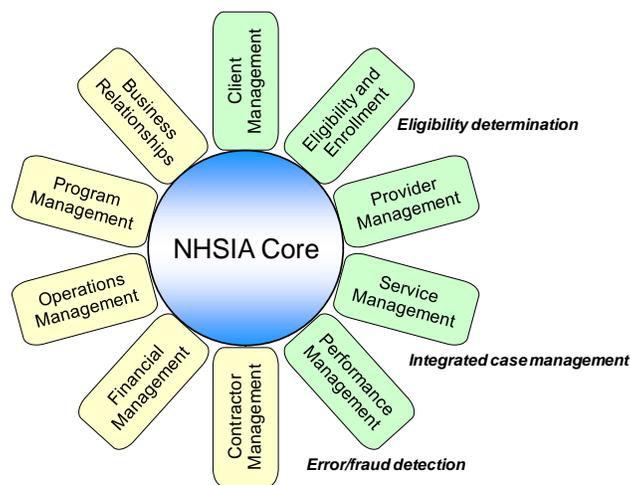


Figure 3-2. NHSIA Core Supports All Business Areas

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

⁷ See the NHSIA Business Viewpoint Description and attachments for more about business areas, business processes, and business activities and their relationships to capabilities. See the NHSIA Capability Viewpoint Description and attachments for more about NHSIA capabilities.

- A service-oriented architecture (SOA) infrastructure in each IT environment that supports human services. The SOA infrastructure provides the foundation for IT service discovery and re-use.
- A set of hubs to share IT services. Information sharing may use NIEM-based standards. The initial shared IT services and information sets are those required to support the 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.

Elements to provide the core capabilities may be implemented in IT environments at different levels of government. The NHSIA Architecture Team drafted a list of core IT services and related interfaces. The NHSIA Jurisdiction Teams will vet and modify this initial list and continue to evolve it over time. For more on the core capabilities, services, and related interfaces, please see the "NHSIA Core" Concepts document.

NHSIA will be implemented over time. The as-is systems comprising NHSIA have been developed over a period of a couple decades or more. It is not feasible to replace them or even modify them all in a few years. Given that it will take some years to accomplish the upgrade, it is not possible to foresee all the changes in laws, regulations, the economy, and technology that will impact the to-be state beyond a few years out. Implementing a core set of capabilities will enable critical information sharing and create an environment that allows new capabilities to evolve more easily. The Internet and World Wide Web are two common, extremely successful examples of this type of approach. Both have underlying architectures that permit expansion into new features and capabilities never envisioned when the architectures were first defined.

3.3 NHSIA System of Systems

NHSIA describes an architecture for an enterprise that extends across multiple independent organizations. The systems comprising NHSIA form a system of systems (SOS). Systems of systems often have characteristics different from a large system comprised of multiple subsystems that are all developed for a single purpose. These characteristics include:

- Operational independence of the individual systems – each system is operated independently to accomplish a useful function on its own
- Managerial independence of the individual systems – each system is funded, developed and managed by independent organizations
- Geographical distribution – systems are not co-located

- Emergent behavior – the full capabilities aren't apparent until the SOS is operational and its components begin to evolve
- Evolutionary development – capabilities are added and improved over time
- Self-organization – doesn't depend on central management
- Adaptation – the SOS can adapt to changes to technical, economic, and other changes over time and remain useful

These characteristics require a different approach to architecting and development than would be possible in a single enterprise where top-down direction and control are possible. Gartner⁸ refers to an approach that can be used in this situation as a “middle-out” architecture approach. The term is to contrast with a top-down or bottom-up approach. The middle-out approach focuses on the interfaces between systems versus the functions and designs of the system. As an example, even if the details of an eligibility system are not known, it is clear that certain information will need to be verified with authoritative sources. So if the national architecture focuses on defining the verification interface, states can build their eligibility system to meet their needs and yet have access to verification services via standard interfaces.

Another characteristic of this approach is that it focuses on defining a limited core of interfaces using open standards in such a way that independent parties can extend, evolve, and adapt the architecture over time.

3.4 Roadmap

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 a manageable effort, the Jurisdiction NHSIA team may initially focus on clearly defining and implementing the NHSIA core capabilities. A multi-year effort is envisioned as illustrated in Figure 3-3.

In the figure, federal government activities are in blue boxes and state government activities are in yellow boxes. 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.

⁸ The Gartner Group, “Understanding EA Approaches: Middle-Out”, Publication ID: G00168166, 18 December 2009.

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. So there can be no single acquisition approach for all of NHSIA implementation. Each state, county, and private organization will need to develop its own plan.

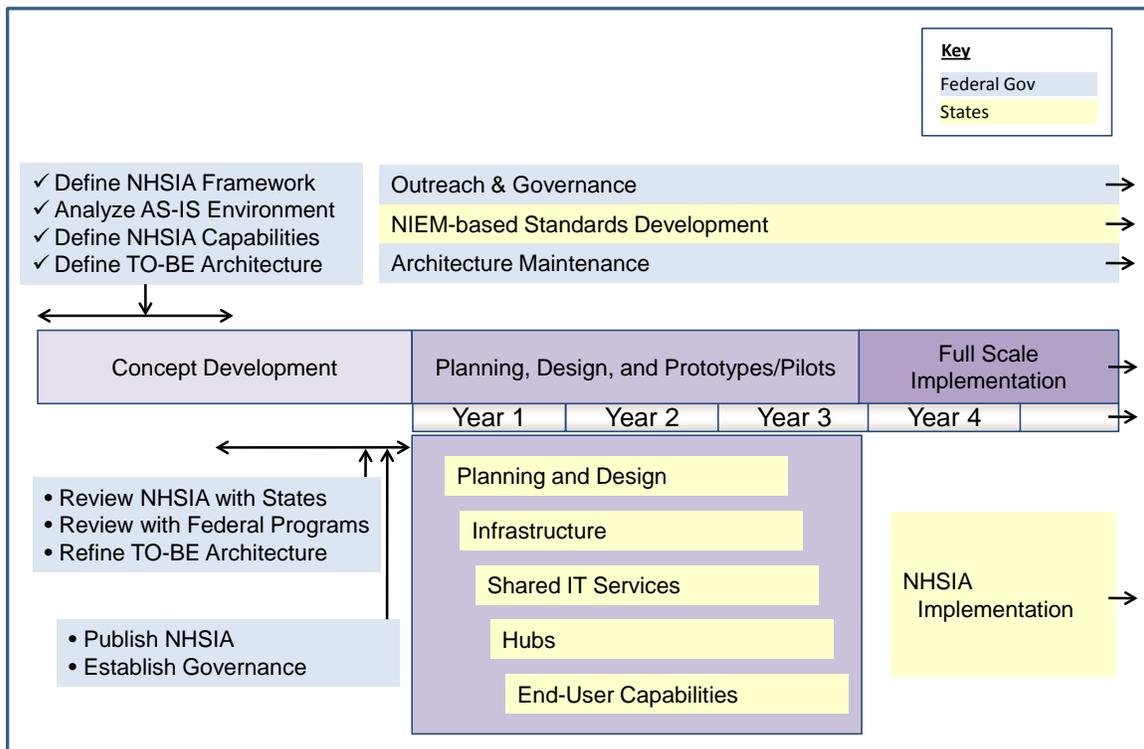


Figure 3-3. Notional NHSIA Roadmap

3.5 Jurisdiction's Steps

Figure 3-4 illustrates the steps recommended for the Jurisdiction NHSIA Team to follow to implement NHSIA:

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

Subsequent chapters in this document describe the steps in detail. The descriptions may seem to imply that adopting NHSIA is an “all or nothing” prospect. This is not the case. A jurisdiction may adopt NHSIA concepts in some areas but not in others. Priorities, problem areas, related initiatives, and resource availability will influence where a jurisdiction focuses.

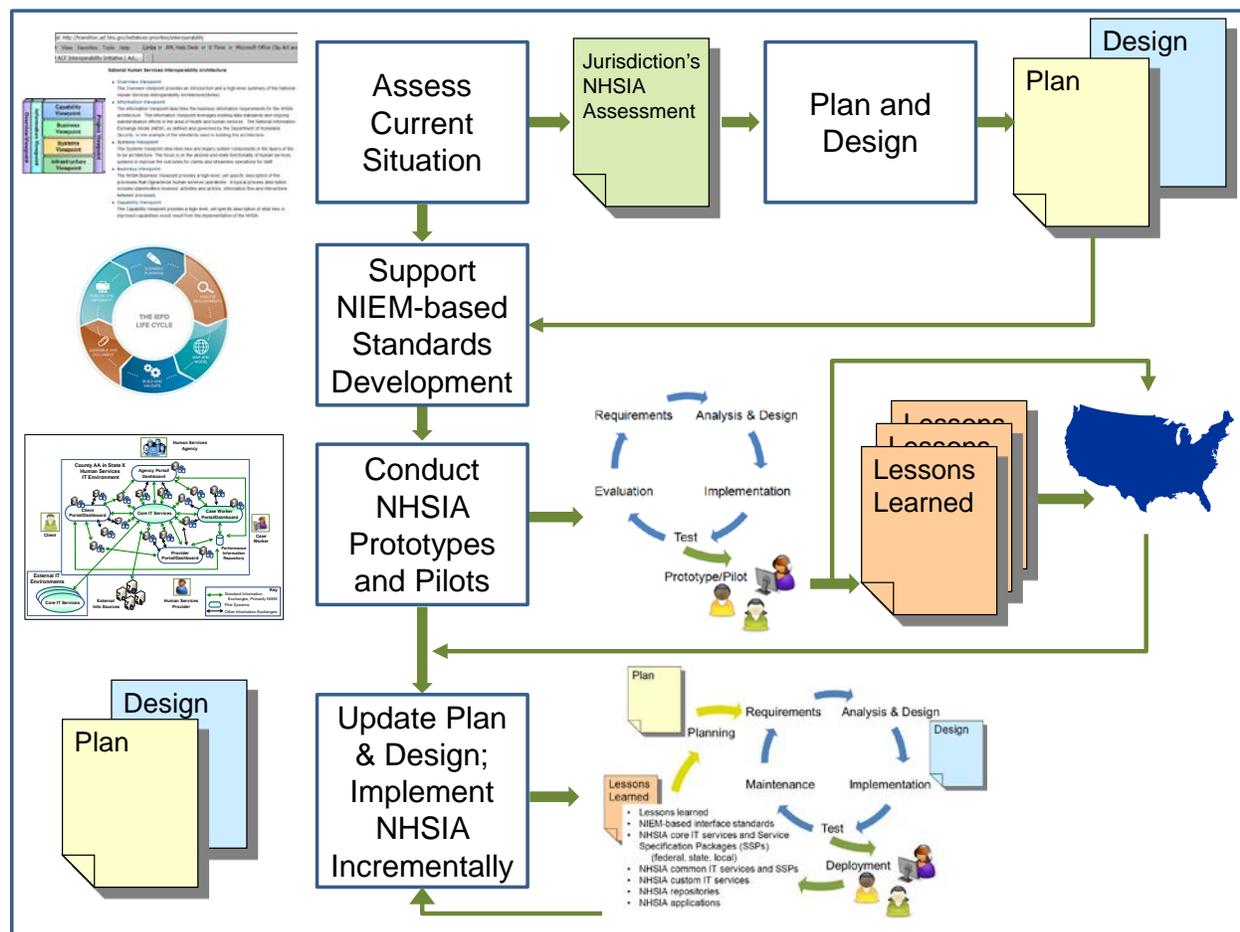


Figure 3-4. Jurisdiction’s Steps to Implement NHSIA

Many aspects of the approach outlined in this document are based on the methodologies recommended in the Global Reference Architecture (GRA). The GRA is “an abstract framework for understanding significant components and the relationships between them within a Service-Oriented Architecture. It lays out common concepts and definitions as the foundation for the development of consistent SOA implementations within the justice and public safety communities.”⁹ NHSIA has adopted many of the GRA concepts and definitions,

⁹ U.S. Department of Justice’s Global Reference Architecture (GRA) Framework, Global Infrastructure/Standards Working Group (GISWG), Version 1.9, April 2011. Available online at <http://it.ojp.gov/globaljra>.

adapting them as needed for the human services community. We encourage jurisdictions to read the GRA documentation and incorporate the concepts. Appendix B – summarizes the GRA documents.

4 Assess Current Situation

The Jurisdiction NHSIA Team should attain a clear understanding of what NHSIA is about and assess where the jurisdiction stands relative to NHSIA's goals, concepts, principles, and the "to-be" architecture described in the NHSIA reference model.

Activities in this step include:

- Review NHSIA documentation available on ACF's Interoperability Initiative website¹⁰ to understand what NHSIA is.
- Determine potential benefits of NHSIA to the jurisdiction. Assess commitment to high-level NHSIA goals, concepts, and principles (see the Overview Viewpoint Description). This might be expressed in a memorandum of understanding/agreement signed by the heads of the agencies, departments, programs, or other entities that will be involved in improving interoperability in order to improve the delivery of human services.
- Assess current environment. We recommend that the Jurisdiction NHSIA Team record their analysis in a brief document that addresses at least these topics:
 - Identify the key stakeholders who should be involved in NHSIA planning and design.
 - Identify the NHSIA capabilities that are already implemented in the jurisdiction. See the Capability Viewpoint Description and detailed Capabilities List. Use the capability scorecard referenced in the Capability Viewpoint Description. A sample scorecard (Scorecard View tab) is in the Capabilities List spreadsheet file.
 - Review the NHSIA generalized business processes and determine potential alignment with existing, more detailed jurisdiction processes. See the NHSIA Business Viewpoint and related Excel Business Model files.
 - Review the draft list of elements that will support the NHSIA core capabilities and determine alignment with the jurisdiction's plans. See the "NHSIA Core" Concepts and related Excel files.
 - How will NHSIA support current business practices or drive change? What aspects of NHSIA are already implemented? What ideas are already part of existing plans? What ideas will motivate change?

¹⁰ Note: The URL for the site is currently: <http://transition.acf.hhs.gov/initiatives-priorities/interoperability>. When ACF completes the migration to their new website the URL is expected to be <http://www.acf.hhs.gov/initiatives-priorities/interoperability>.

- Which capabilities are most important to the jurisdiction? Perhaps add a column to the Scorecard to record priorities.
- Which capabilities will be easiest to achieve?
- Which capabilities present the biggest challenge?
- What are the overarching business problems across human services in the jurisdiction that NHSIA can help to solve?¹¹
- What ongoing or planned projects should be considered/revised/coordinated with NHSIA implementation?
- What information is already being shared? Do additional partners need the information? Which information exchanges would be of most value to the jurisdiction? Who are the partners in those information exchanges?
- Given the way information is managed currently, what are the main challenges associated with expanded information sharing? What model for "harmonizing" (i.e., reconciling, consolidating, integrating, optimizing, etc.) data from different systems and/or different organizations makes sense?

¹¹ The set of overarching business problems can be used in the Plan and Design phase to set the drivers and objectives that will steer the identification of core IT services. Factors for high-priority business problems may include those identified in Appendix C of the "NHSIA Core" Concepts document, based on the GRA model. Note that NHSIA is not a panacea to solve every challenge faced by human services practitioners. NHSIA focuses on comprehensive eligibility determination and information sharing across programs and agencies, improved delivery of services, prevention of fraud, and better outcomes for children and families through improved interoperability of business processes and information technology.

5 Plan and Design

Based on the assessment of the current situation, the Jurisdiction NHSIA Team should develop a plan for beginning to implement NHSIA and a top-level design for how NHSIA elements will fit into the existing information systems architecture. The jurisdiction should follow their standard program planning and systems engineering practices. The jurisdiction may develop a Planning Advance Planning Document (APD), prepare an Implementation APD, update one or more existing APDs [i.e., submit an APD Update (APDU)], or capture the plan and design in some other document(s). The jurisdiction's efforts to implement NHSIA should initially focus on the elements required to support the core capabilities, IT services, interfaces, and repositories. The jurisdiction should also consider planning NHSIA prototype or pilot activities to test the concepts and experiment with implementation models.

Activities in this step include:

- Identify jurisdiction champion(s) for NHSIA
- Identify team leadership
- Establish governance
 - Participants
 - Objectives
 - Processes, procedures
- Form the implementation team
- Develop a program plan, including these topics:
 - Needs, objectives, scope, stakeholders. Base on output from Assess Current Situation.
 - Activities, schedule, deliverables, resources. Prioritize according to desired capabilities, high payoff areas, opportunities for funding, and participation in pilot activities. Note: The activities and schedule should define phases for incremental implementation, starting with the core capabilities and one or more high-value end-user capabilities that utilize the core foundation. In each phase, add new capabilities.
 - Changes to existing/new business processes.
 - Jurisdiction's recommendations about NHSIA core elements; see Appendices A and B of the "NHSIA Core" Concepts.
 - IT services the jurisdiction will develop or procure. Identify which IT services will be coordinated with other jurisdictions (common IT services), and those which federal agencies are best positioned to provide. The process outlined in Appendix B of the "NHSIA Core" Concepts suggests a systematic method for evaluating which functions are candidates for service-enabling.

- Legacy systems that will be modified or replaced to adopt NHSIA concepts.
- Proposed budget.
- Cost allocation.
- Describe a jurisdiction architecture that is compliant with NHSIA.
 - Infrastructure. Refer to NHSIA Infrastructure Viewpoint Description.
 - System components (applications and services). These may be existing components that will be modified or new components to be developed or procured. Refer to NHSIA Systems Viewpoint Description and Services Matrix.
 - Identify major information-sharing interfaces. Refer to NHSIA Information Viewpoint Description and Information Exchanges spreadsheet.
 - Establish a process to address enterprise-wide data management issues (e.g., reconciling data from multiple sources, consolidating redundant data into a single authoritative source, and other issues identified in the Assess Current Situation step).
 - Establish a process that involves instrumenting the activities associated with providing human services to embed the collection and evaluation of performance information.

Again, note that NHSIA is not an “all or nothing” prospect. A jurisdiction may adopt NHSIA concepts in some areas but not in others. Priorities, problem areas, related initiatives, and resource availability will influence where a jurisdiction focuses.

6 Support NIEM Standards Development

There is growing support for developing NIEM-based information exchanges. If well-defined legacy interfaces exist, and those who will share the information have long-standing working relationships, there may be little value in expending the effort to develop a NIEM-based exchange. However, if there is a new requirement, a significant change to an existing interface, or if new working relationships are needed, the jurisdiction should consider basing the new interface on NIEM. There is value in mapping data elements used in legacy interfaces to NIEM in order to develop a commonly understood vocabulary.

Thus, throughout the jurisdiction's NHSIA effort, one or more members of the Jurisdiction NHSIA Team may participate in relevant NIEM working groups. The working groups will develop information exchange package documentation (IEPDs) for NHSIA-related information exchanges. Each jurisdiction involved will assist in creating and adopting the interfaces to meet the specific information sharing needs; some tailoring by the jurisdiction may be required. See the [NIEM](#) site for more information about NIEM.

This page intentionally blank

7 Prototype or Pilot Parts of NHSIA

Some jurisdictions may choose to prototype or pilot elements of NHSIA before embarking on full deployment. For example, NHSIA core elements and one or more selected end-user capabilities may be prototyped or piloted¹² to validate the architecture and demonstrate operational utility. A state's prototype or pilot might include all or some IT services, repositories, and interfaces to support the NHSIA core capabilities. A prototype or pilot project could also include implementing one or more end-user business capabilities. This means the state's pilot project might include:

- Establishing a service-oriented infrastructure
- Establishing selected core IT services
- Establishing a county and/or state hub
- Establishing at least one end-user capability such as:
 - Eligibility and enrollment
 - Case management
 - Performance management
 - Fraud detection

The first three items put in place core information system elements to support the core capabilities. The fourth item uses the core elements and demonstrates their utility in delivering capability to end-users.

The details of how the prototype and pilot projects will be conducted and organized must be worked out as funding and organizational issues are resolved. Some jurisdictions may have already accomplished many aspects of one or more of the envisioned projects.

Ultimately, the NHSIA capabilities are intended to be implemented within each state and/or county. However, for the prototype and pilot projects, a jurisdiction may choose to implement a subset of capabilities. It may be that a jurisdiction will focus on some element for which they have the foundation in place and that is of most value to them.

As part of the prototype and pilot activities, we encourage participants to share lessons learned. If a pilot is successful, the design and implementation may be re-usable by others. We encourage states to form working groups with each other to

¹² By prototype, we mean an implementation that may not have all the features necessary to be put into operational use. By pilot, we mean an operational pilot. In other words, it is a pilot which implements a capability in an operational environment and is actually used to support operations.

facilitate sharing lesson learned. The NHSIA Architecture Team may use the lessons learned and model designs/implementations to update the architecture documentation.

7.1 Establish the Infrastructure

NHSIA proposes that each jurisdiction establish an IT infrastructure that is generic in the sense that it could support nearly any type of application, not limited to human services. This infrastructure would use state-of-the-practice IT concepts which inherently support interoperability. These concepts include:

- Service-oriented architecture
- Enterprise service bus
- Server and storage virtualization
- Cloud computing
- Infrastructure security

More specifically, the Global Reference Architecture (GRA) is recommended as the approach to be used in implementing SOA. The Global Federated Identity and Privilege Management (GFIPM) approach is recommended as an important component of the infrastructure security architecture. The GFIPM approach will enable single sign-on and attribute-based access control. The NHSIA Infrastructure Viewpoint and NHSIA Security White Paper provide additional details.

A state that plans to prototype/pilot some end-user NHSIA capability would probably need to establish at least a limited part of this infrastructure as a foundation.

7.2 Establish Core IT Services

NHSIA defines a limited set of IT services that comprise the foundation for the core capabilities. The core capabilities require IT services to

- Find and get basic and/or summary information about key entities (person, case, provider, and program)
- Verify information against authoritative sources
- Support a set of repositories to facilitate selected data aggregation and analysis

These requirements suggest **core IT services** in these categories:

- Deployed in local and/or state IT environments, depending on how human services are administered and managed:

- Master Person Index (MPI). To locate records about persons in human services systems.
- Person. To share basic information about a person.
- Verification of person information. To verify information about the person from local and/or state authoritative sources.
- Case. To share summary information about cases related to persons who are receiving or have received human services.
- Summary of cases. To share a summary of cases (potentially, gathered from different organizations and associated with different programs) related to a person.
- Program information. To share local-level or state-level information about human services programs, including reporting local-level performance information to the state level or state-level performance information to the federal government.
- Provider registry. To locate records about human service providers.
- Provider. To share basic information about human service providers.
- Verification of provider information. To verify information about the provider from local- or state-level authoritative sources.
- Deployed at the federal level
 - Verification of person information. To verify information about a person or human services provider from national- or federal-level authoritative sources.
 - Verification of provider information. To verify information about the provider from national- or federal-level authoritative sources.
 - Program information. To share federal-level information about human services programs.

7.3 Establish a County and/or State Hub

NHSIA defines a hub as a place within the service-oriented IT environment that is used to host services, applications, and information to be shared externally. The hub may also contain other elements that are only shared internally. The NHSIA pilot activities might include implementing hubs at the county and/or state level.

To make shared IT services easily accessible across different organizations, programs, and jurisdictions, one NHSIA core concept is that a hub is aware of the existence of other NHSIA hubs. Sharing hub information should be part of the pilot projects.

7.4 Establish End-User Capability

The prototype/pilot projects should include implementing all or some IT services, repositories, and interfaces to support the core capabilities. A prototype or pilot project should also include implementing one or more end-user business capabilities. Enabling someone to use a single sign-up process for multiple human services is one example. By “single sign-up”, we mean that integrated eligibility/enrollment services permit a client to sign up for multiple human services programs via a single application and enrollment process. A portal/dashboard that gives access to multiple functions is another example/model for providing end-user business capabilities. The prototype and/or pilot projects may build one or more portals/dashboards that will use core IT services to provide useful capabilities to end users:

- Client
- Case worker
- Provider
- Human services program manager

For example, the portal function may provide the client with an access point to link to any online human services Web site within the jurisdiction serving them. The dashboard function may provide a summary of any program information relevant to human services they have applied for or are receiving. The dashboard would provide drill-down and drill-through capabilities.

Figure 7-1 illustrates one example for the elements in a pilot implementation. The figure shows a pilot deployment of the caseworker portal/dashboard and related core IT services. In practice, a county may choose to pilot a different portion of the capabilities shown or may implement an end-user capability that uses NHSIA core capabilities without using the dashboard/portal approach. This example configuration represents a county that has its own IT environment and in which state-supervised human services are administered at the county level. Some interfaces may be based on standards.

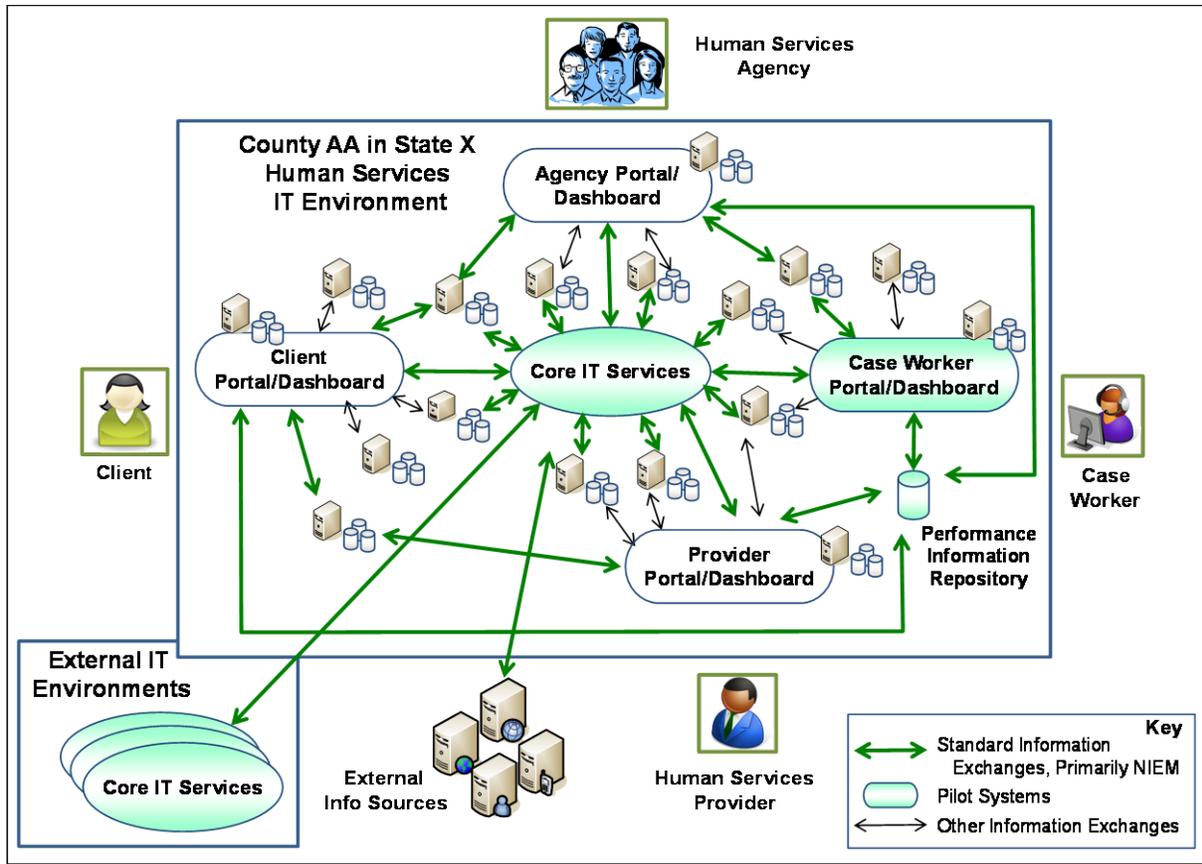


Figure 7-1. Example County Pilot Deployment of NHSIA

This page intentionally blank

8 Update Plan and Design; Implement NHSIA Incrementally

This final step takes inputs from all previous steps the jurisdiction has taken on its NHSIA journey. This step is iterative, as the jurisdiction incrementally deploys the design; see Figure 8-1. Each cycle corresponds to a phase in the NHSIA plan. In each iteration cycle, the process begins with considering lessons learned from the previous cycle, then updating the plan and design, implementing new capabilities, and deploying the new capabilities to end-users. Through state working groups, one jurisdiction may also leverage lessons learned, designs, and implementation of IT services from other jurisdictions.

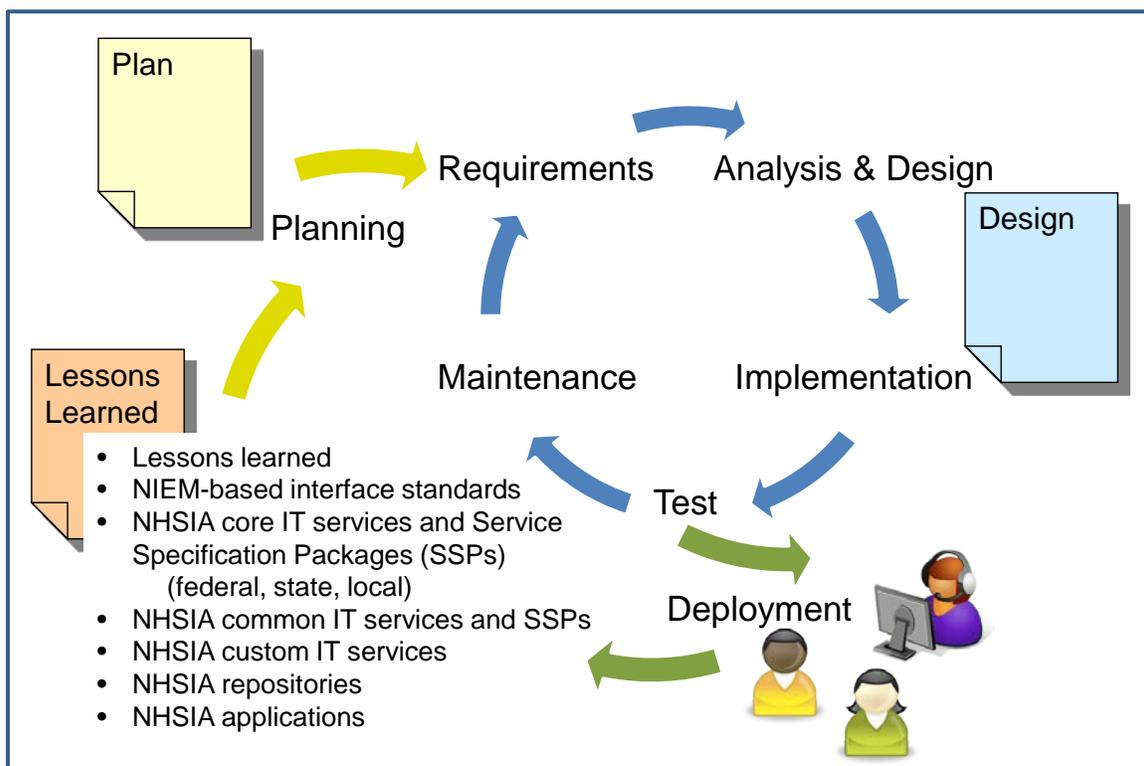


Figure 8-1. Iterative Process for Incremental Implementation

8.1 Update NHSIA Plan and Design

Before embarking on full-scale NHSIA implementation or starting a new cycle of incremental deployment, the jurisdiction will revisit and update their plan and design for how to deploy and enhance information systems that comply with NHSIA. During this process, the Jurisdiction NHSIA Team will work with the end-user communities and implementation teams to determine specific capabilities and associated information system requirements to be incorporated in the current deployment cycle. The deployment activities should take into account the maturity

of NIEM-based standard interfaces, IT services available from others, and designs/implementations for repositories and applications shared by others.

The plan for a deployment cycle will reflect actual resource availability and external factors that influence priorities, schedules, and technical considerations. For instance, if the state is implementing a cloud architecture to support all IT environments, the plan for deploying NHSIA elements should include how to best utilize that technology. The jurisdiction may transition gradually from its current systems and move towards full implementation according to its own needs, priorities, and resources.

8.2 Implement NHSIA Incrementally

Earlier we introduced the concept of common, core, and custom IT services. Implementing NHSIA starts with laying the foundation. This means the jurisdiction would implement the elements that support the core capabilities. Next the jurisdiction uses that foundation to deliver capabilities to end-users. This means the jurisdiction will implement common and custom elements. The implementation would be planned in increments.

NHSIA, like the GRA¹³, is built on several architecture principles that apply in this system of systems environment:

- **Independence of Information Sharing Partners.** Human services information sharing should accommodate a large number of independent information sharing partners at the federal, state, local, and tribal levels of government.
- **Scalability.** Human services information sharing should provide useful guidance to integrated enterprises of all sizes, from small operations with a few participants, to larger processes that reach across local, state, tribal, and federal boundaries.
- **Diversity of Data Source Architectures.** Human services information sharing should accommodate data sources and partner systems that differ widely in software, hardware, structure, and design.
- **Agility.** Human services information sharing should accommodate changes in policy, business rules, information flow, and partner system implementation without forcing investments or changes in unrelated systems or exchanges.
- **Reuse and Sharing of Assets.** Human services information sharing should promote the use of existing system interfaces, information exchanges, and infrastructure to support new business requirements.

¹³ These principles are based on the [Global Reference Architecture Framework](#), Version 1.9, April 2011

- **Alignment with Best Practices and Experience.** Human services information sharing should reflect concepts and mechanisms that have proven viable in actual, real-world information exchange scenarios; the architecture should reflect the experiences of both public- and private-sector information exchange implementation projects.

These principles guide the jurisdiction to

- Define system interfaces that focus on the system functionality or information to be shared, not on how organizations design, deploy, or operate their systems.
- Base information sharing mechanisms on open industry standards rather than proprietary solutions.
- Work with partners to reach agreement on information sharing and allow independent approaches for other aspects of information systems and operations.
- Follow a modular, incremental approach to deployment.
- Adopt technologies and approaches (e.g., cloud computing) that support business needs and facilitate re-use and sharing resources.
- Adopt industry standards and employ implementations available from the marketplace based on needs and resources.
- Describe IT services clearly and make them readily discoverable.
- Minimize implementation dependencies between systems that share information.
- Separate the logic of information exchange (e.g., the routing and transforming of messages that flow between partners) from the logic of line-of-business systems.
- Share lessons learned, designs, and implementations so that future decisions can be based on practices that have proven effective.

8.2.1 Elements to Support Core Capabilities

Implementing the core capabilities will provide a foundation for other elements of NHSIA. The jurisdiction may evolve from its current systems and move towards full implementation according to its own needs and priorities. These core elements are discussed below:

- SOA
- Single sign-on and attribute-based access control
- Repositories
- Hubs

8.2.1.1 SOA

One key aspect of the NHSIA core is to deploy a service-oriented architecture (SOA). SOA is a methodology for systems development and integration where functionality is grouped around business processes and packaged as interoperable services¹⁴. SOA also describes an IT infrastructure that allows different applications to exchange data with one another as they participate in business processes. The aim is a loose coupling of services with operating systems, programming languages and other technologies that underlie applications.

SOA separates functions into distinct units, or services, which are made accessible over a network so that they can be combined and reused in the production of business applications. These services communicate with each other by passing data or by coordinating an activity between two or more services.

With respect to the NHSIA infrastructure, a Service-Oriented Architecture, then, is an architectural style for creating an IT infrastructure that exploits the principles of service orientation to achieve a tighter relationship between the business and the information systems that support the business. These information systems may be used by different organizations/agencies.

Figure 8-2 illustrates a notional IT environment for a county that adopts NHSIA. There may be several IT environments in a large county.

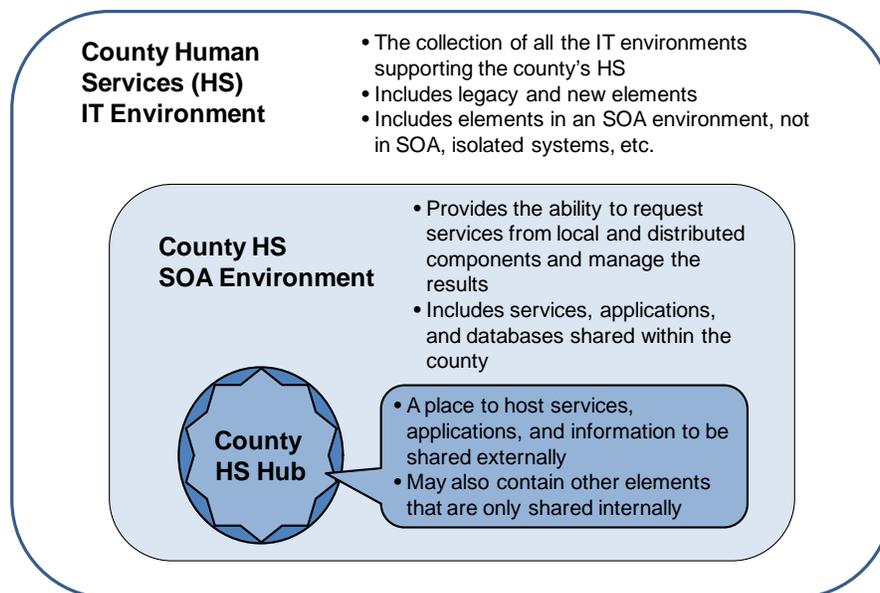


Figure 8-2. Notional IT Environment for a County that Adopts NHSIA

¹⁴ Erl, Thomas (2005). *Service-oriented Architecture: Concepts, Technology, and Design*. Upper Saddle River: Prentice Hall PTR.

- The large white box represents the collection of all the IT environments that are involved with supporting human services in the county. It includes all aspects of all IT environments, both legacy elements and those deployed to support NHSIA concepts. It includes the service-oriented environment as well as others that are not service-oriented.
- The middle light blue box is the service-oriented IT environment. It is a subset of the county HS IT environment. The SOA IT environment provides the ability to request services from local and distributed components and manage the results. It includes IT services, applications, and databases that are shared within the county.
- The blue circle contains the hub. It is a subset of the HS SOA environment. The hub is used to host IT services, applications, and information to be shared externally. The hub may also contain other elements that are only shared internally.

Elements to provide the NHSIA capabilities will be implemented in IT environments at different levels of government.

Following the GRA standard for describing IT services¹⁵ makes it possible to understand, use, and consume those services across jurisdictions.

The jurisdiction may decide to start by moving a few legacy applications to the SOA environment. A family of applications that use the same set of data or serve the same stakeholders might be good starting candidates.

8.2.1.2 Single Sign-on and Attribute-based Access Control

NHSIA stakeholders need to be able to efficiently access and securely share and protect information. While organizations are likely to have invested significantly in securing their own environments, NHSIA complicates an already complicated area by bringing users and data together in a new, shared environment. Because of this, NHSIA implementation must provide mechanisms to authenticate users who will access the environment, must authorize their admittance into the environment, and must control the applications and information to which those individuals have access. NHSIA implementation must ensure that data are communicated into and out of the shared environment securely and that data are adequately secured and protected. The NHSIA white paper on security¹⁶ provides useful guidance. NHSIA has adopted the principles of the GRA's Global Federated Identity and Privilege Management (GFIPM) approach. Following the GFIPM model, jurisdictions can

¹⁵ [Global Reference Architecture Service Specification Guidelines](#), Working Draft Version 1.0.0, December 2011.

¹⁶ NHSIA Security White Paper, Draft version D0.2, June 2012.

communicate a standard set of elements and attributes about a federation user's identities, privileges, and authentication.

“The GFIPM metadata and framework support the following three major interoperability areas of security in the federation:

- *Identification/Authentication - Who is the end user and how were they authenticated?*
- *Privilege Management - What certifications, clearances, job functions, local privileges, and organizational affiliations are associated with the end user that can serve as the basis for authorization decisions?*
- *Audit - What information is needed or required for the purposes of auditing systems, systems access and use, and legal compliance of data practices?”¹⁷*

Single sign-on (SSO) addresses the cumbersome situation of logging on multiple times to access different resources. After NHSIA is implemented, users should not be required to maintain separate sets of logon credentials to access their local and shared resources. When users must remember numerous passwords and IDs, they are more likely to take shortcuts in creating them that could leave them open to exploitation.

In SSO, a user provides one ID and password per work session and is automatically logged on to the required systems or applications. The advantages of SSO include having the ability to use stronger passwords, easier administration of changing or deleting the passwords, and less time to access resources. Federation takes SSO to the next level, providing a secure, standard, Internet-friendly way to share identity among multiple organizations and applications. Users sign on once (the SSO) using their standard network login. Their identity is then transparently and securely shared with the requested application, thereby removing the additional login requirement. Since the employee's organization authenticates him or her, and the application provider can verify the authenticity of the provided federated identity, application passwords are obviated and users are able to access applications.

Single sign-on streamlines the user's experience in accessing IT systems. Human services workers will require access to shared applications and resources. Human services clients will require access to their own information and information about programs. Data integrity and confidentiality must be ensured. Sharing information about the user's roles, rights, and privileges in a secure manner enables single sign-on and attribute-based access control.

¹⁷ [Global Federated Identity and Privilege Management](#), accessed February 27, 2012.

To promote service integration and ensure privacy compliance, the jurisdiction may need to adjust policy, practices and procedures, and system controls.

Policy considerations include:

- Existing laws and regulations
- Information-sharing responsibilities and options for clients
- Information-sharing and protection responsibilities for workers and organizations
- Information-sharing and protection responsibilities for systems
- Memorandum of understanding (MOU) to allow information sharing between agencies based on
 - Who needs the information
 - What information
 - Purpose and intended use of the information
- Federated identity and privilege management

Practices and procedures should address:

- Manage user (person and system) identity
 - Provision user (enroll user in the system and assign or adopt credentials). This should be allowed only if there is a valid MOU with the user's organization.
 - Authenticate user (confirm that a user corresponds to the username provided)
 - Authorize access (grant access to IT service and/or resource based on authentication)
 - Account for access (log access and authorization for audit trail)
- Establish a common authorization "form" that client signs
 - Standard list of categories of information
 - Standard list of purposes for sharing information
 - Client selects which categories can be shared for which purposes
- Systems allow attribute-based access to IT service and/or resource
 - User attributes – to control types of access the user has to which resources
 - Entity attributes – to define the role each sharing partner plays
 - Resource attributes – to define the type of resource; includes category for information
 - Action attributes – to define what actions are permitted by a user against a resource

Key system controls include:

- Provide single sign-on of users to authenticate user and gather attributes
- Record authentication activities (failed and successful attempts)
- Before granting access to information
 - Check for valid user authentication
 - Check that user attributes align with resource attributes for data to be accessed
 - Check that user attributes align with resource attributes for purpose for access to that data
 - Check that action attributes align with user’s intended action
 - Check that the specific client has authorized access to that data for that purpose
- Encrypt all personally-identifiable information
- Record access activities to support audit trail

Table 3 illustrates an example of the kind of information that might comprise a common client authorization “form”. The form should be stored electronically. It may also include other attributes, such as: when the authorization expires, with what organizations the information may be shared for the specified purpose, etc. Only a few high-level notional information categories and information sharing purposes are shown in this example. Jurisdictions and programs should collaborate to establish a common set of categories and purposes for sharing information.

Table 3. Notional Common Client Authorization "Form"

Sharing Purpose Information Category	Determine eligibility	Plan services	Etc.
Name	Y	Y	
Contact	Y	Y	
Demographics	Y	Y	
Employment	Y	Y	
Family and references	Y	Y	
Finances	Y	N	
Health	N	N	
Legal/court	Y	N	
Client history	Y	Y	
Etc.			

The concept is that, within the bounds of existing laws and regulations, each human services client selects which categories of information about himself or herself can be shared for different purposes. The IT systems would need to accommodate the client's authorization when sharing information.

Figure 8-3 illustrates, at a high-level, the major steps to use the federated user credentials, rules for controlling access to information and IT resources, and the common client authorization. This is one possible way to use those elements to ensure privacy compliance. The figure shows Jane Doe authorizing limited access to data about her that is stored in the Shared Person Data set for specific purposes. For purposes of this example, we assume Jane Doe filled in the common client authorization form as shown in Table 3.

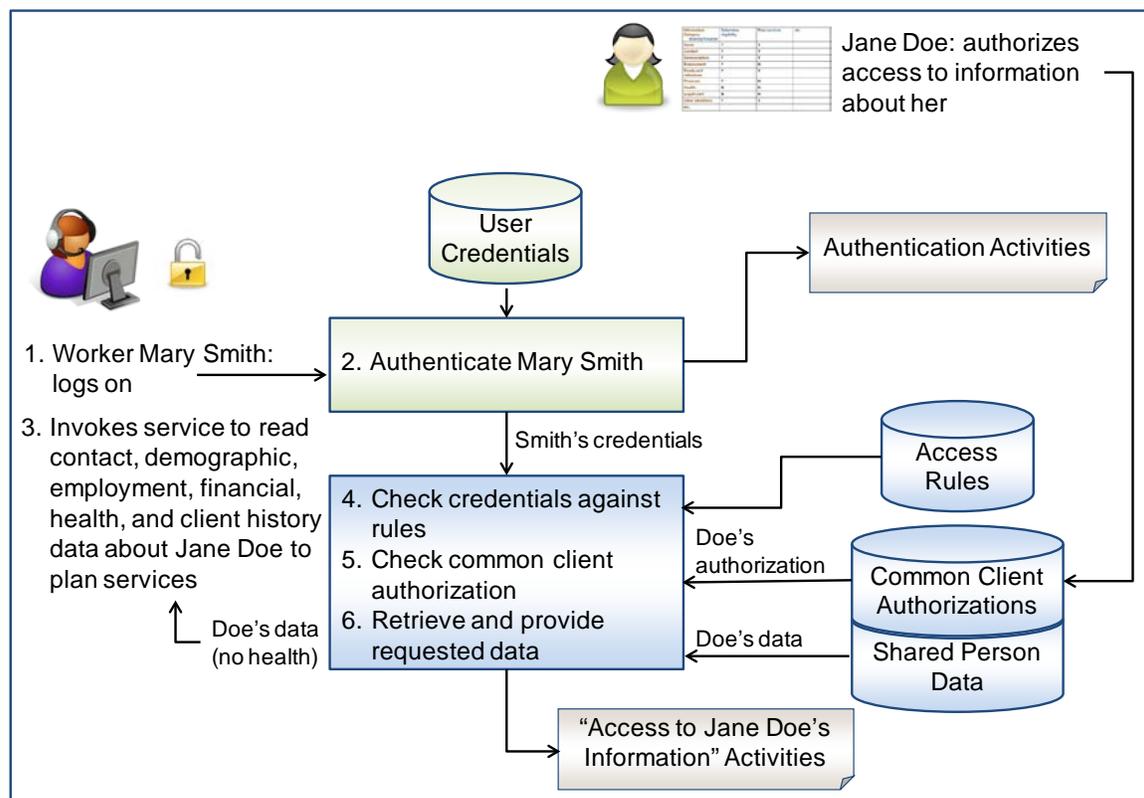


Figure 8-3. Notional Access Control

- In step 1, case worker Mary Smith is trying to plan services for Jane Doe and logs on to her HS system.
- In step 2, her logon is authenticated. Part of that process retrieves her privileges. She is authorized to plan services and access relevant data for that process. The system records the successful authentication.
- In step 3, Mary requests a set of data about Jane Doe, including financial and health data.

- In step 4, the system checks Mary's credentials against the access rules and confirms that Mary can plan services and access relevant data, including financial and health data.
- However, according to the Jane Doe client authorization form, she does not want someone who is planning services to view her financial or health data. So, in step 5, when the system checks the common client authorization for Jane Doe, it recognizes that it must withhold the financial and health data.
- In step 6, the system retrieves the requested data based on Mary Smith's credentials, the access rules, and the limitations imposed by Jane Doe's common client authorization. The system records accessing Jane Doe's information. The system provides the information to Mary Smith, minus the financial and health data. Because the information is personal about Jane Doe, it is encrypted as it leaves the boundaries of its owning organization.

This example illustrates some of the major aspects of using single sign-on and attribute-based access control to ensure privacy compliance according to both regulations and the client's wishes. Providing these foundational capabilities enables the jurisdiction to support end-users from different organizations who are performing a variety of functions.

8.2.1.3 Repositories

Human services workers and clients require access to various sets of information and to IT services. Jurisdictions will implement repositories that authorized users and user systems can access. As part of fully implementing the NHSIA core capabilities, jurisdictions will implement a Performance Information Repository (PIR) to collect operational information from the jurisdiction's human services activities so the information can be used to assess performance across, potentially, multiple agencies, organizations, and programs.

NHSIA's notion of instrumenting human services activities implies implementing a shared, integrated PIR. Jurisdictions can use today's information technology to improve operational processes and systematically collect, aggregate, analyze, and visualize information in meaningful ways to enable in-depth understanding of the performance of processes and programs at all levels. Jurisdictions may use this information to explore the applicability and usage of improved evidence-based practices. They may also use this information to detect waste, fraud, and abuse to ensure that benefits are efficiently provided only to those intended and that positive outcomes are maximized. The PIR allows the jurisdiction to aggregate information using analytics tools for the purpose of state and federal reporting. Figure 8-4 illustrates the NHSIA conceptual architecture for performance management via performance information repositories.

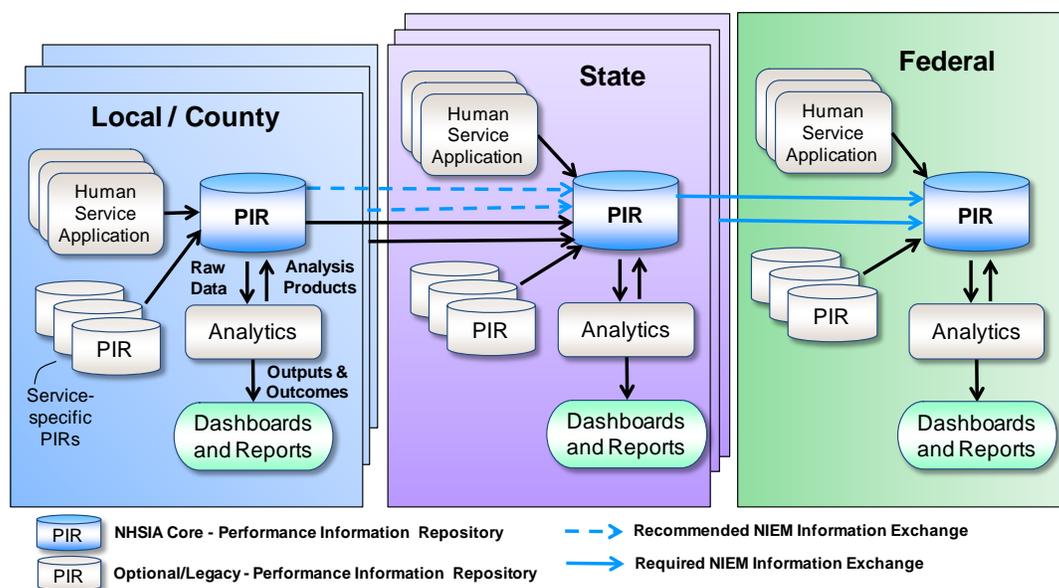


Figure 8-4. Reference Model: Performance Information Repositories

The gray PIR canisters represent service-specific PIRs. These may or may not exist in a given jurisdiction or for a given program. Analytics tools process the raw data and generate products including metrics and reports related to outputs and outcomes. Analytics are enhanced by the integration of performance information across human services programs and agencies/organizations. The connections between the local/county-level integrated PIRs and the state-level integrated PIR represent sharing whatever information the state needs to perform its analysis. Similarly, the connections between the state-level integrated PIRs and a federal-level integrated PIR represent sharing whatever information the federal government needs to perform its analysis. Integrating the PIRs at the state and federal levels should reduce duplication of effort and data reporting, and also enable more meaningful analysis. A PIR may be implemented as a "virtual" structure that is physically several different databases.

The "NHSIA Core" Concepts document¹⁸ describes these other kinds of "repositories" as well.

- IT service registry
- Master person index
- Provider registry
- Hub catalog

¹⁸ "NHSIA Core" Concepts, Draft version D0.3, September 2012.

8.2.1.4 Hub

A hub is a place within the service-oriented IT environment that is used to host services, applications, and information to be shared externally. The hub may also contain other elements that are only shared internally. Each jurisdiction will establish a hub in its SOA. At a minimum the hub will host the IT services and the repositories that are required to support the core capabilities. See Appendix A in the “NHSIA Core” Concepts.

To share a service, the IT service provider will develop formal documentation that describes the capabilities made available through the service. As suggested in the GRA¹⁹, NHSIA recommends that this Service Specification Package (SSP) define the:

- Capabilities the service provides and semantics of the service by representing its behavioral model, information model, and interactions. This includes specifying what business capabilities the service provides, roles and responsibilities of the partners using and providing the service, and the information exchanges that provide the information flows. The specification states general assumptions about the service that apply (e.g., storing messages in a log file or acknowledging messages) to support interoperability.
- Policies that constrain the use of the service. This includes references to MOUs, service-level agreements, security policies, etc.
- Service interface that provides a means of interaction with the service. This includes the specific protocols, commands, and information exchange by which actions are initiated on the service. Directly from the GRA Service Specification Guidelines:

“A service interface is what a system designer or implementer (programmer) uses to design or build executable software that interacts with the service. That is, the service interface represents the “how” of the interaction. Since the service interface is the physical manifestation of the service, best practices call for service interfaces which can be described in an open-standard, machine-referenceable format (that is, a format which could be automatically processed by a computer).”²⁰

The Service Specification Package provides stakeholders with an understanding of the structure and functionality of the service and the applicability of its implementation interface rules (policies). It gives service consumers the information necessary for consuming a particular service, and service providers the information

¹⁹ [Global Reference Architecture \(GRA\) Service Specification Guidelines](#), Global Justice Information Sharing Initiative, Working Draft V 1.0.0, December 2011.

²⁰ Ibid.

necessary for implementing the service in a consistent and interoperable manner. Details of the contents of the information exchanges will be documented via NIEM IEPDs or other equivalent interface descriptions (if an exchange is not based on NIEM).

To make shared IT services easily accessible across different organizations, programs, and jurisdictions, one NHSIA core concept is that a hub is aware of the existence of other NHSIA hubs. Figure 8-5 illustrates one way that information about the hubs could be shared — via a catalog hosted in a nationally-accessible hub. Other models are possible.

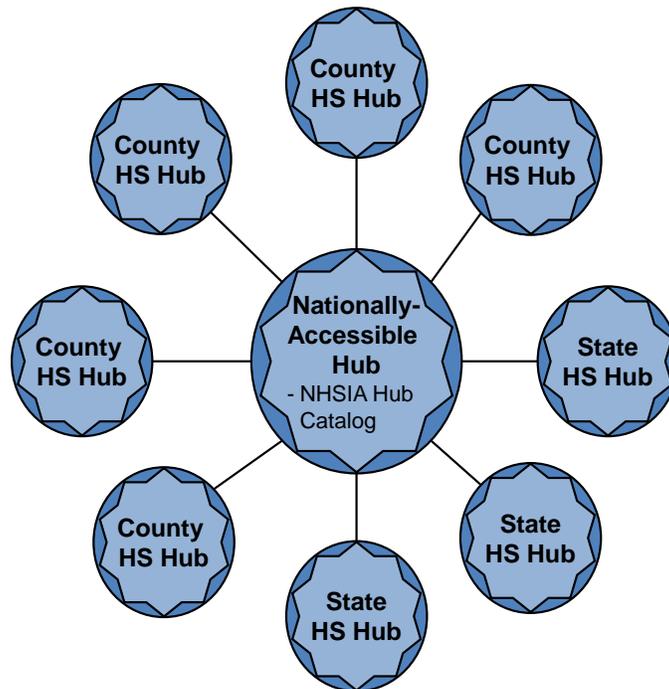


Figure 8-5. A Catalog Is One Way to Make Information about Hubs Available

8.2.2 Common Elements

As described earlier, common elements are those that support cross-jurisdiction and/or cross-program or agency information sharing. Some of the common elements have been designated as “core” because they provide foundational capability. Other common elements are just as important. Following the process for identifying IT services outlined in Appendix B of the “NHSIA Core” Concepts, the Jurisdiction NHSIA Team will review and revise the draft list of common IT services that the NHSIA Architecture Team started. We recommend that NHSIA interstate working groups collaborate to fully identify and characterize the common IT services and related interfaces. NIEM teams will develop IEPDs for the common interfaces.

The Jurisdiction NHSIA Team will choose which common elements to implement in each NHSIA implementation cycle. The common elements should support the end-user capabilities planned for the cycle.

8.2.3 Custom Elements

Each jurisdiction will implement unique custom elements. Custom elements may adopt or adapt NIEM-based standards for interfaces. Custom elements may maintain some aspects of the repository information that is shared across organizations within the jurisdiction. Custom elements may follow common element models but tailor them in some way.

8.3 Share with Other Jurisdictions

When a deployment cycle is completed, we recommend that the jurisdiction share lessons learned, IT services, repository designs, and information about applications with others. To the extent possible, the jurisdiction could share actual implementations, possibly by participating in interstate working groups. This promotes re-use and minimizes the cost of deploying NHSIA for everyone. The Jurisdiction NHSIA Team should keep this goal in mind during procurement activities.

9 Recap

Two diagrams presented earlier summarize the activities described in this document.

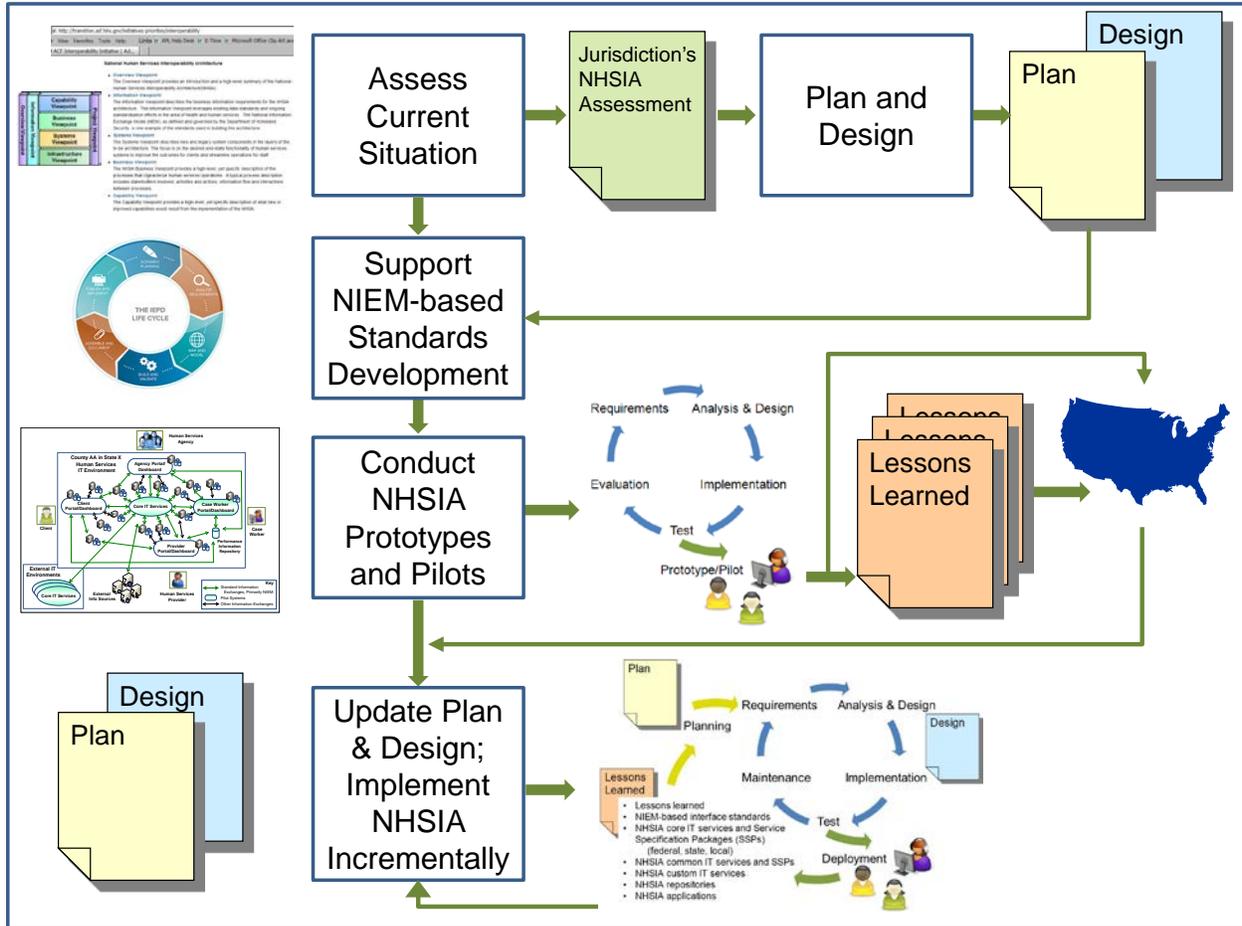


Figure 9-1. Jurisdiction’s Steps to Implement NHSIA (repeated)

A jurisdiction that is aligning its human services information systems will follow the steps shown in Figure 9-1.

- **Assess Current Situation.** Record the analysis in a brief document, labeled Jurisdiction NHSIA Assessment in the figure.
- **Plan and Design.** Prepare or update project plans to reflect incorporating NHSIA concepts. Update or prepare APD if seeking federal support. Prepare or update enterprise-wide architecture to reflect NHSIA concepts.
- **Support NIEM Standards Development.** Join working groups to develop information exchange standards based on NIEM.
- **Prototype or Pilot Parts of NHSIA.** Help to validate NHSIA and deploy core foundation.

- Update Plan and Design; Implement NHSIA Incrementally. Incrementally deploy more capabilities in a way that is consistent with NHSIA. See Figure 9-2.

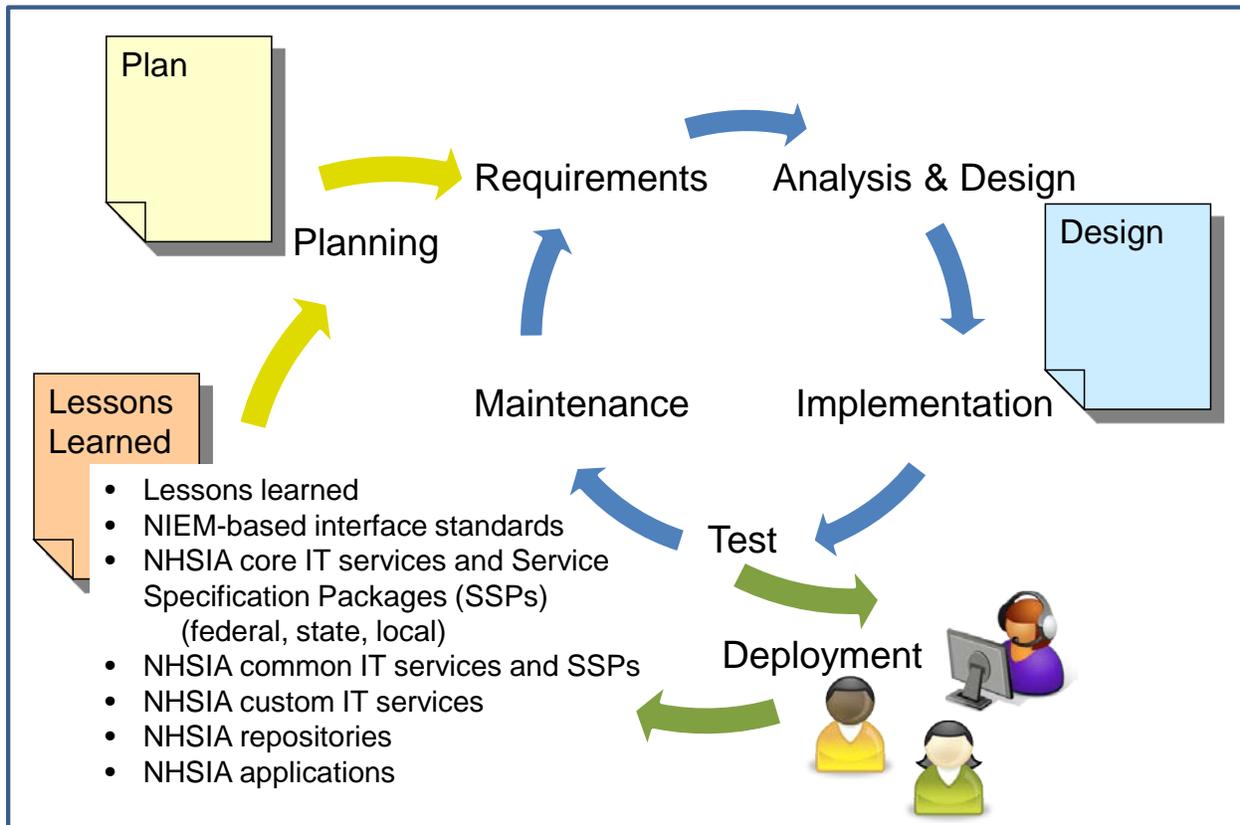


Figure 9-2. Iterative Process for Incremental Deployment (repeated)

The “Update Plan and Design; Implement NHSIA” step takes inputs from all previous steps the jurisdiction has taken on its NHSIA journey. This step is iterative, as the jurisdiction incrementally deploys the design. Each cycle corresponds to a phase in the NHSIA plan. In each iteration cycle, the process begins with considering lessons learned from the previous cycle, then updating the plan and design, implementing new capabilities, and deploying the new capabilities to end-users. Through interstate working groups, one jurisdiction may also leverage lessons learned, designs, and implementation of IT services from other jurisdictions.

10 References

- 1) National Human Services Interoperability Architecture (NHSIA) documents, prepared by Johns Hopkins University for the Administration for Children and Families. Available online at ACF's Interoperability Initiative website. The URL for the site is currently: <http://transition.acf.hhs.gov/initiatives-priorities/interoperability>. When ACF completes the migration to their new website the URL is expected to be <http://www.acf.hhs.gov/initiatives-priorities/interoperability>. See Figure 1-2 or Appendix A – Accessibility Appendix for a list of documents.
- 2) National Information Exchange Model. Information available online at <http://www.niem.gov/>
- 3) IEPD Clearinghouse. Available online at <http://www.it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm>
- 4) U.S. Department of Justice's Global Reference Architecture (GRA) Framework, Global Infrastructure/Standards Working Group (GISWG), Version 1.9, April 2011. Available online at <http://it.ojp.gov/globaljra>.
- 5) U.S. Department of Justice's Global Reference Architecture (GRA) Frequently Asked Questions, issued September 2011. Available online at <http://it.ojp.gov/globaljra>.
- 6) U.S. Department of Justice's Global Reference Architecture (GRA) Service Specification Guidelines, Global Justice Information Sharing Initiative, Working Draft V 1.0.0, December 2011. Available online at <http://it.ojp.gov/globaljra>.
- 7) U.S. Department of Justice's Global Reference Architecture (GRA) Guidelines for Identifying and Designing Services, Global Infrastructure/Standards Working Group (GISWG), Version 1.1, May 2011. Available online at <http://it.ojp.gov/globaljra>.
- 8) U.S. Department of Justice's Global Federated Identity and Privilege Management, Introduction. Accessed February 27, 2012. Available online at <http://it.ojp.gov/gfipm>.
- 9) Thomas Erl, Service-oriented Architecture: Concepts, Technology, and Design, Upper Saddle River: Prentice Hall PTR, 2005.
- 10) National Association of State Chief Information Officers (NASCIO), Capitals in the Clouds, The Case for Cloud Computing in State Government Parts I-IV, 2011-2012. Available online at <http://www.nascio.org/publications>.

This page intentionally blank

Appendix A – Accessibility Appendix

This section contains accessible versions of figures and tables in this document. Table and figure numbers that appear here correspond to versions that appear earlier in this document.

Figure 1-2. NHSIA Viewpoints with Artifacts
(Converted to bulleted list under each viewpoint)

Overview Viewpoint Artifacts

- O-01-OverviewViewpointDescription-D0.3
- O-As-IsReport-D0.1
- O-As-IsAppendixA-D0.1
- White Papers
 - O-ClientAndCaseManagement-D0.2
 - O-ElectronicHealthRecordsApplicability-D0.1
 - O-Eligibility-D0.2
 - O-MasterPersonIndexServices-D0.2
 - O-Rules-D0.2
 - O-Security-D0.2
 - O-PerformanceInformationRepositories-D0.3

Information Viewpoint Artifacts

- I-01-Information Viewpoint Description-D0.2
- I-02-Conceptual Data Model-D0.2
- I-03-Information Exchanges-D0.2
- I-Data Dictionary and NIEM Mapping-D0.1
- I-List of Relevant Standards-D0.1

Capability Viewpoint Artifacts

- C-01-CapabilityViewpointDescription-D0.3
- C-02-CapabilitiesList-D0.3
- C-03-NHSIAPerformanceReferenceModel-D0.2
- C-04-PRMAppA-SelectedHHSPerformanceMeasures-D0.2

- C-05-PRMAppB-MajorSystemsDatabasesACF-D0.2
- C-06-PRMAppC-PerformanceIndicatorsACF-D0.2
- C-07-PRMAppD-PerformanceIndicatorsStateCountyCityDashboards-D0.2

Business Viewpoint Artifacts

- B-01-BusinessViewpointDescription-D0.2
- B-02-ProcessesMappedToHumanServiceDomains-D0.2
- B-03-ClientManagementBusinessProcesses-D0.2
- B-04-EligibilityAndEnrollmentBusinessProcesses-D0.2
- B-05-ProviderManagementBusinessProcesses-D0.2
- B-06-ServiceManagementBusinessProcesses-D0.2.
- B-ScenariosAndVignettes-D0.1

Systems Viewpoint Artifacts

- S-01-SystemsViewpointDescription-D0.2
- S-02-Services-D0.2
- S-03-ApplicationsMappedToBusinessProcesses-D0.2

Infrastructure Viewpoint Artifacts

- F-01-InfrastructureViewpointDescription-D0.1

Project Viewpoint Artifacts

- P-01-ProjectViewpointDescription-D0.3
- P-02-NHSIACoreConcepts-D0.3

Appendix B – Global Reference Architecture Documents

The Global Reference Architecture (GRA) initiative is managed by the U.S. Department of Justice, Office of Justice Programs, Justice Information Sharing. The GRA “provides a comprehensive blueprint for implementing interoperable data sharing services and capabilities”²¹.

GRA provides many resources. Table 4 summarizes the contents of several documents. Readers may also find other documents of interest on the GRA Website (<http://it.ojp.gov/globaljra>). In a future iteration, the NHSIA Architecture Team may update NHSIA documents as indicated in the right-hand column to incorporate many GRA concepts more directly.

²¹ <http://www.it.ojp.gov/default.aspx?area=nationalInitiatives>

This page intentionally blank

Table 4. GRA Documents

GRA Document	Overview	NHSIA Document to be updated
<p>GRA Framework v1.9 http://it.ojp.gov/docdownloader.aspx?ddid=1223</p>	<p>Conceptual framework for SOA that is based on an industry standard, the OASIS SOA Reference Model, which was developed by a committee of industry and government SOA experts, including some of the GISWG members who authored the GRA. The Framework defines a set of key concepts in a standard way, so that across the country, justice practitioners and their industry partners can adopt a consistent vocabulary for communicating about SOA. The framework also provides a jumping-off point for the rest of the broader reference architecture, by identifying areas where the community needs more thorough standards and guidelines.</p>	<p>Architecture principles already included in Project Viewpoint Description, chapter 8.</p> <p>NHSIA Overview Viewpoint may be updated to directly include GRA principles and concepts.</p> <p>Infrastructure Viewpoint may be updated to include additional material from chapter 4, Concepts and Relationships, and chapter 6, Elaboration of Service Interaction.</p>
<p>GRA Guidelines for Identifying and Designing Services v1.1 http://it.ojp.gov/docdownloader.aspx?ddid=1171</p>	<p>A methodology for identifying what services—exchange points—a jurisdiction should develop to solve some identified business problem.</p>	<p>Concepts already included in “NHSIA Core” Concepts, Appendix B.</p>

GRA Document	Overview	NHSIA Document to be updated
GRA Service Specification Guideline, Working Draft v1.0.0 http://it.ojp.gov/docdownload.aspx?ddid=1215	A standard for describing services so they can be used, understood, and consumed across jurisdictions. Provides formal, standardized means for using, creating, and understanding Service Specifications and Service Specification Packages. Provides a method for describing and documenting the scope, in addition to the functional and technical requirements of a service in sufficient detail to allow service providers to develop interoperable service implementations and service consumers to review, select, and use these services by referring to the same specification.	The Project Viewpoint Description refers to this document when describing, at a high level, what jurisdictions should do to document their shared IT services. The Systems Viewpoint may be updated to include additional details about describing services.
GRA Execution Context Guidelines v1.1 http://it.ojp.gov/docdownload.aspx?ddid=1170	Recommended requirements for infrastructure necessary to support SOA. Provides guidelines to practitioners overseeing the implementation of a SOA regarding the implementation of infrastructure to support reachability, willingness, awareness, and intermediaries.	Infrastructure Viewpoint may be updated to include additional material about this GRA concept.
GRA Information Sharing Enterprise Statement of Participation v1.1 http://it.ojp.gov/docdownload.aspx?ddid=1172	Provides a reference model framework of expectations and obligations for those entities participating in any state, local, regional, or tribal information sharing enterprise. Provides a general set of obligations, rules, and remedies that support the information sharing environment, as well as promoting interoperability, agility and reuse of conformant information services.	Service agreements, identity and privilege management, acceptable use, audit, and privacy and data quality concepts are already included in Project Viewpoint Description, chapter 8. This document may be updated to include additional concepts and guidelines.

GRA Document	Overview	NHSIA Document to be updated
GRA Information Sharing Enterprise Service-Level Agreement v1.1 http://www.it.ojp.gov/docdownloader.aspx?ddid=1327	Provide a sample Service-Level Agreement (SLA),	none

This page intentionally blank