Provider Directories Initiative Overview

January 20, 2012

Table of Contents

1 **Introduction to the S&I Framework**

•What is unique about the S&I Framework

2 **Introduction to Provider Directories Initiative**

•Initiative Success Metrics
•Consensus Statistics

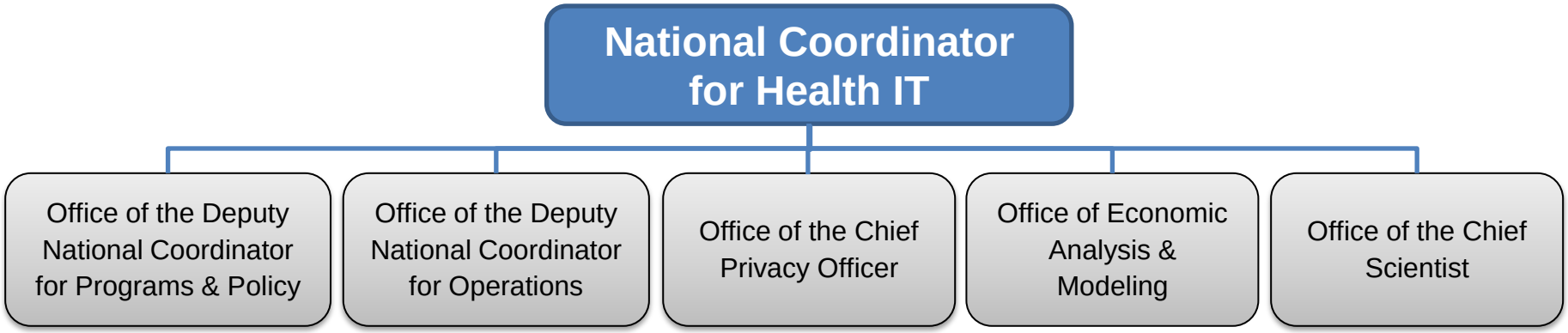
3 **Use Case 1 - Certificate Discovery for Direct Project**

•Introduction to Certificate Discovery for Direct Project
•Value Proposition for the Workgroup
•Timeline
•Example User Story
•Development of Recommended Hybrid Approach
•Summary of Analysis underlying Proposed Solution
•DNS/LDAP Hybrid Approach
•DNS/LDAP Hybrid Approach Implementation Guide
•Next Steps

4 **Use Case 2 - Electronic Service Information Discovery**

•Introduction to Electronic Service Information Discovery
•Value Proposition for the Workgroup
•Timeline
•Example User Story
•Development of the 2 Data Model
•Data Model Overview
•X12N 274 and LDAP/HPD Standard Mapping
•X12N 274 and LDAP/HPD Standard Mapping

Introduction to the S&I Framework



Office of Policy & Planning

Office of Standards & Interoperability

Office of Provider Adoption Support

Office of State & Community Programs

- The Standards and Interoperability (S&I) Framework is a forum – enabled by integrated functions, processes, and tools – for implementers and experts to establish harmonized standards that enable healthcare information exchange
- It represents one investment and approach adopted by the Office of Standards & Interoperability to fulfill its charge of enabling harmonized interoperability specifications to support national health outcomes and health care priorities, including Meaningful Use and the Nationwide Health Information Network

What is unique about the S&I Framework Approach?

- **S&I Framework Approach:**
  1. Creates a collaborative, coordinated, incremental standards process
  2. Guided by ONC, with input from Federal Advisory Committees
  3. Enabled and led by an open community of industry participants who are interested in solving real world problems

- **Value created through this approach:**
  - Solves real-world issues to enable health information exchange
  - Harnesses the expertise and passion of the community to solve problems
  - Empowers the community by providing tools, coordination, and harmonization to create the best solutions for interoperability and standards adoption
  - Creates a model as well as tangible work products for future community led efforts

Introduction to the Provider Directories Initiative

The Provider Directories Initiative consists of two complementary workgroups dedicated to the same outcome: *Secure exchange of health information across organizational boundaries*

1. **Certificate Discovery for Direct Project (Use Case 1)**

   Enable healthcare participants to look up digital certificate information to facilitate secure exchange of information through Direct Project

2. **Electronic Service Information Discovery (Use Case 2)**

   Help HIEs/EHRs/PDs to enable query and response for electronic service information including electronic addresses, with corollary benefits to data governance, PD instantiation, and HIE/EHR development and deployment

Initiative Success Metrics

- The number of Provider (and Certificate) Directories receiving queries from and sharing messages with EHR systems
- The number of EHR systems that have been certified to support Provider (and Certificate) Directories messages
- The number of providers and other authorized entities that can look up information from Provider and Certificate Directories
- Number of implementations of core set of data elements to support queries to Provider Directories by EHR vendors, State HIEs, HISPs and other mediators of exchange
- The level of improvement in providers' ability to achieve MU criteria dependent on secure messaging and exchange of information beyond Stage 1
- Number and level of detail for unambiguous certification requirements of EHR systems to support provider directory messages

Consensus Statistics

Consensus is a core value of the S&I Framework. To achieve consensus in Provider Directories all legitimate views and objections were reviewed and an endeavor to resolve them was taken. Listed below are the outcomes :

Deliverable	"Yes" Votes	Consensus Dates	Committed Organizations	Consensus Link
Certificate Discovery for Direct Project Implementation Guide	10	12/5/2011 - 1/9/2012	Allscripts, Cequs, EnableCare, Newborn Coallition, Oz Systems, Cerner Corp, RelayHealth, Siemens Health Care, Techsant Technologies,	Link
Electronic Service Information Data Model	12	11/18/2011 - 12/4/2011	ABILITY Network, Accredited Standards Committee X12, Allscripts, Cequs, EnableCare, Health Market Science, IBM, MedAllies, Oz Systems, Shape HITECH, Siemens Health Care	Link
ESI Data Model Master Mapping Spreadsheet	10	1/6/2012 - 1/20/2012	Accredited Standards Committee X12, Cequs, EnableCare, Health Market Science, Holon Solutions, IBM, MedAllies, Oz Systems, Shape HITECH, Siemens Health Care	Link

Use Case 1
Certificate Discovery for Direct Project

Introduction to Certificate Discovery for Direct Project

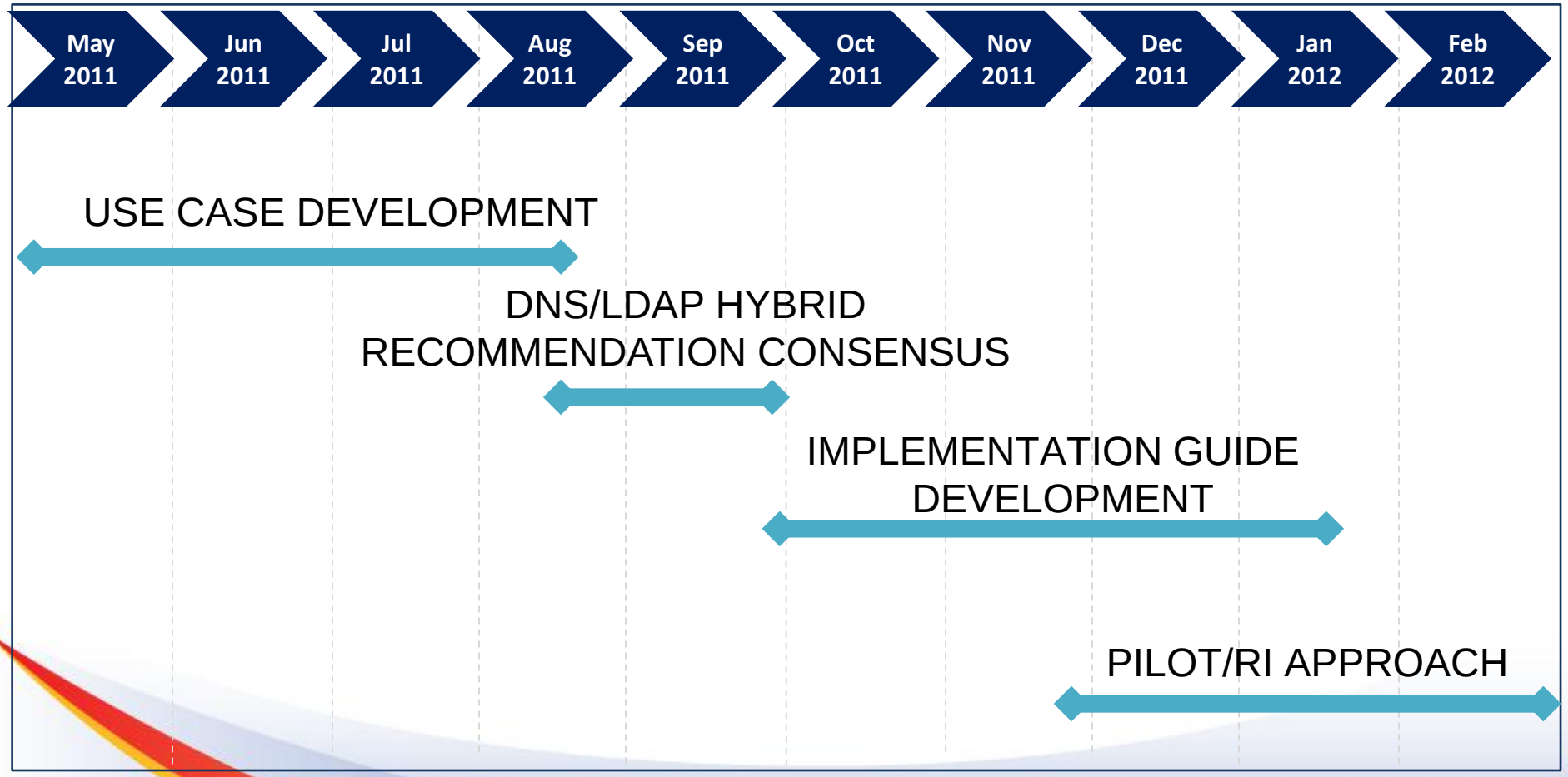
- **The Use Case 1 workgroup focused on three health IT objectives:**
  1. The ability for providers and other authorized entities to retrieve digital certificate(s) to facilitate secure exchange of health information
  2. A standardized query mechanism for Certificate Directories that can be adopted by EHR vendors, State HIEs, HISPs and other mediators of exchange
  3. The standardization and simplification of the implementation of interfaces to query Certificate Directories
- **The work group's efforts were led by volunteer leads Dr. Ken Pool, MD (OZ Systems) and Srinivas Koka (Techsant Technologies, LLC)**

Value Proposition for Workgroup

Members of the health care community will benefit from the Certificate Discovery for Direct Project work products because they:

- Instruct providers on how to publish their public digital certificate on a network
- Instruct providers on how to quickly and easily locate one another's public digital certificate
- Enable vendors to develop electronic health record software that supports the querying and publishing of public digital certificates
- Protect the privacy of patients by enabling the secure electronic transfer of medical data

Timeline


May 2011
Jun 2011
Jul 2011
Aug 2011
Sep 2011
Oct 2011
Nov 2011
Dec 2011
Jan 2012
Feb 2012
USE CASE DEVELOPMENT
DNS/LDAP HYBRID RECOMMENDATION CONSENSUS
IMPLEMENTATION GUIDE DEVELOPMENT
PILOT/RI APPROACH

Example User Story

The following user story illustrates the type of transactions that the Use Case 1 work products will enable:

A doctor needs to send a patient's records to a specialist. ***The doctor uses the specialist's email address to find the specialist's public digital certificate.*** *The doctor uses the digital certificate to encrypt the records before sending them as a secure email attachment.*

When the specialist receives the email, he saves the attachment and decrypts the records before meeting the patient. A recipient without the correct private digital certificate cannot decrypt the attachment, so the patient's private medical records would remain secure even if the email fell into the wrong hands.

Development of Recommended Hybrid Approach

The Use Case 1 workgroup investigated currently available options for an open and universally accessible approach to discovering S/MIME digital certificates using only the Direct address. The investigation focused on two specific, highly deployed technologies – DNS and LDAP.

The hybrid approach to discovery of digital certificates is based on the findings of this investigation. This hybrid approach ensures:

- The digital certificate can be obtained if located in a DNS CERT record
- The digital certificate can be obtained if located in an LDAP implementation
- Existing DNS implementations that do not support CERT can facilitate locating the digital certificate
- Data contained in LDAP implementations by health care organizations that store S/MIME certificates can contribute to this use case

Summary of Analysis underlying Proposed Solution

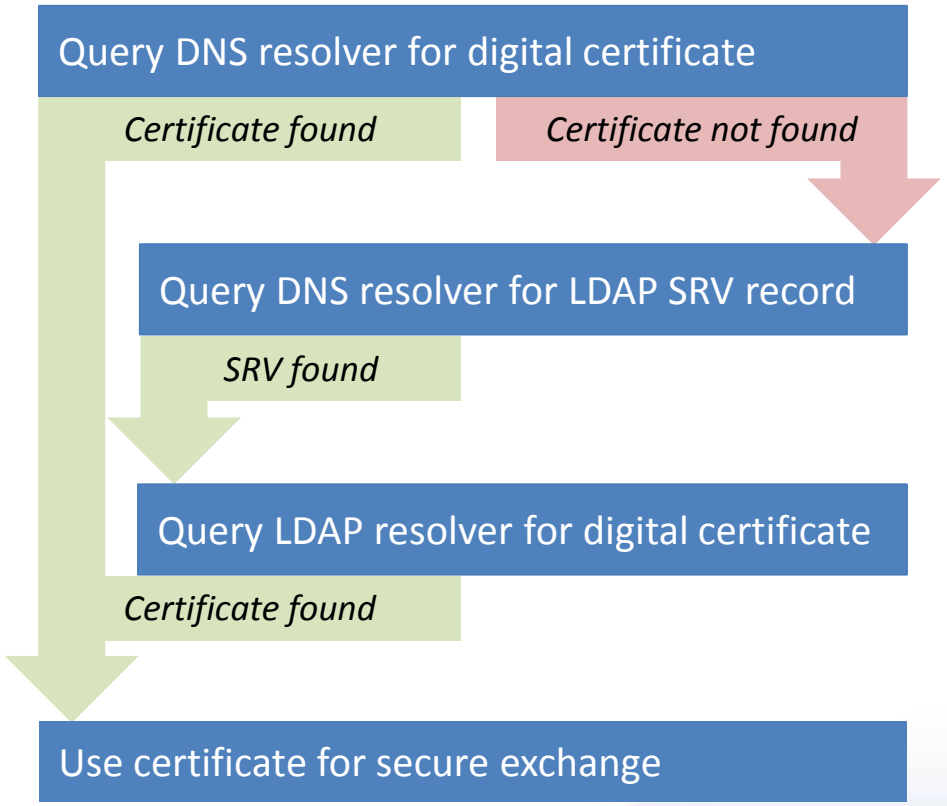
Resolver	Findings
DNS	• Supports Certificate Discovery to the extent required so far by Direct Project pilots • Provides for easy federation and replication of certificate data • A significant number of DNS servers do not support CERT records
LDAP	• Used for certificate discovery in a significant number of organizations • Well-established tools for large organizations and large databases • Some concerns that LDAP does not have broadly demonstrated federation or universal accessibility as currently deployed
DNS + LDAP	• S&I initiative community has updated implementation guidance • Direct Project Reference Implementation Workgroup believes the work required is minimal and complementary • Two Direct Project communities intend to pilot this solution over Q1 2012

DNS/LDAP Hybrid Approach

- **Consensus that DNS for certificate distribution** is an effective part of the solution due to its availability, centralized roots, and replication capability

- **Consensus that LDAP should be supported as the fail-over mechanism** since a large community of organizations have DNS implementation that will not support certificate discovery

Direct Project Reference Implementation



DNS/LDAP Hybrid Approach Implementation Guide

The Use Case 1 workgroup expanded their findings and DNS/LDAP hybrid approach recommendation into an Implementation Guide that provides specific technical guidance on:

- Publishing and discovering LDAP services using the DNS SRV record.
- Querying an LDAP service for digital certificate discovery using anonymous binding for a specific Direct Project address.

The Implementation Guide enables providers and others to electronically obtain the digital certificate of a desired destination to support secure transfer of health information.

Click here to view the guide:

Next Steps

- The Certificate Discovery for Direct Project workgroup will present their work to the HIT Standards Committee (HITSC) for approval.
- Pending HITSC approval, ONC will pilot and test the technical findings of the workgroup.
- The Implementation Guide will be released to the public for testing, review, and use.

Use Case 2
Electronic Service Information Discovery

Introduction to Electronic Service Information Discovery

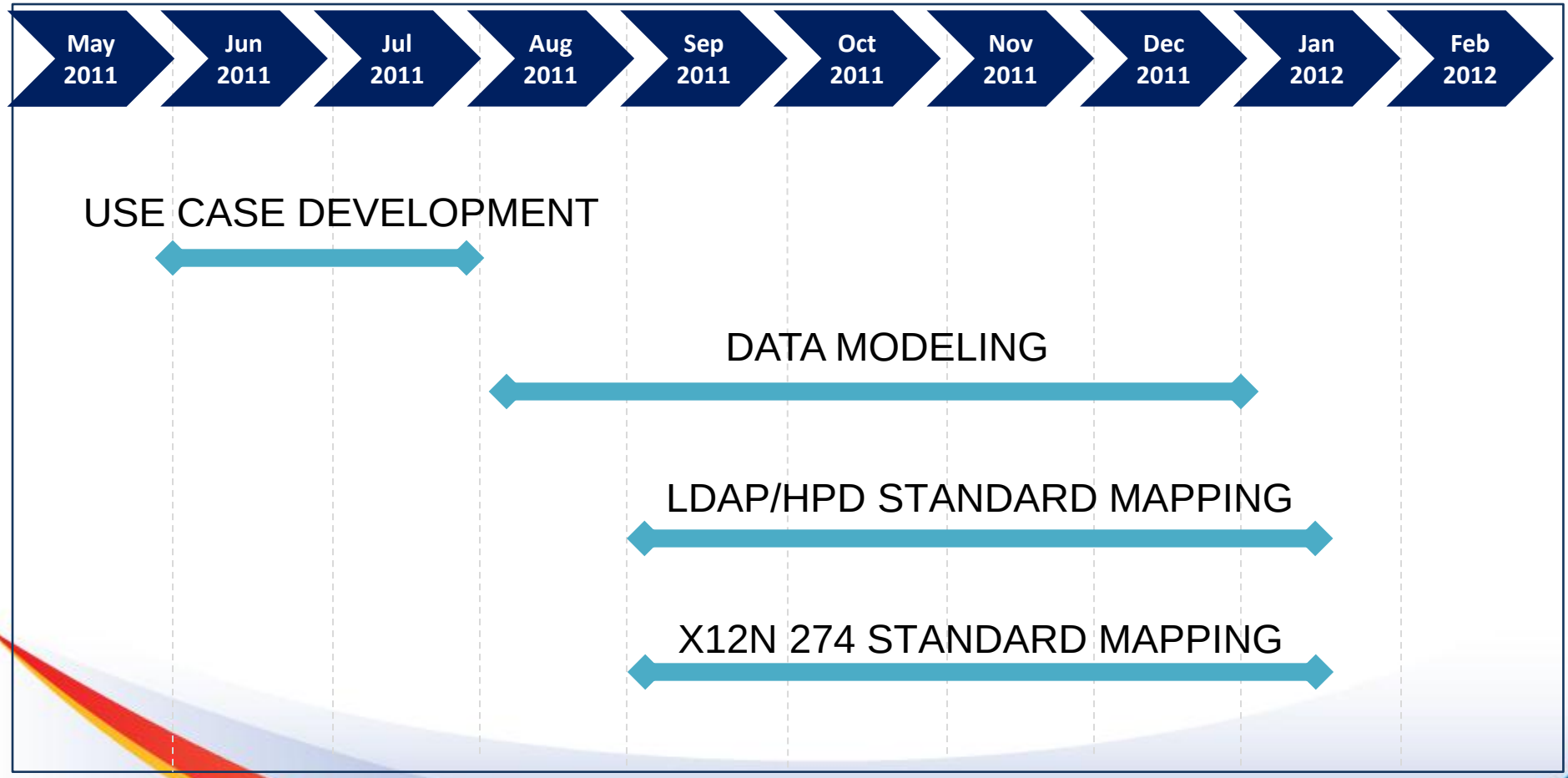
- **Electronic Service Information (ESI)** is the information reasonably necessary to define an electronic destination and its ability to receive and consume a specific type of information, including the destination's electronic address, message framework, payload specification, and required security artifacts
- **The Use Case 2 workgroup focused on three health IT objectives:**
    1. The ability for providers and other authorized entities to look up ESI to facilitate the secure exchange of health information
    2. The development of a core set of data elements to support queries to Provider Directories to retrieve ESI including electronic addresses that can be adopted by EHR vendors, State HIEs, HISPs and other mediators of exchange
    3. The ability for Direct Project implementations to use a Provider Directory to discover Direct Addresses and digital certificates
- **Led by volunteer leads Robert Dieterlie (EnableCare), Karen Whitting (IBM), and Gail Kocher (BlueCross BlueShield Association)**

Value Proposition for the Workgroup

Members of the health care community will benefit from the Electronic Service Information Discovery work products because they:

- Enable vendors to develop directory software that supports the querying and publishing of email addresses, digital certificates, and supported electronic medical records
- Enable providers to quickly and easily locate one another's digital security information
- Protect the privacy of patients by enabling the secure electronic transfer of medical data

Timeline


May 2011
Jun 2011
Jul 2011
Aug 2011
Sep 2011
Oct 2011
Nov 2011
Dec 2011
Jan 2012
Feb 2012
USE CASE DEVELOPMENT
DATA MODELING
LDAP/HPD STANDARD MAPPING
X12N 274 STANDARD MAPPING

Example User Story

The following user story illustrates the type of transactions that the Use Case 2 work products will enable:

A doctor needs to send a patient's medical records to a specialist, but does not know her email address. ***The doctor uses limited information such as the specialist's last name and the organization she works for, to search for and obtain her email address, public digital certificate, and a list of the types of records that the specialist accepts****.*

The doctor generates an appropriate record, encrypts it using the public digital certificate, and sends it to the electronic address. The specialist receives the encrypted record and uses her private digital certificate to decrypt it before meeting the patient. A recipient without the correct private digital certificate cannot decrypt the attachment, so the patient's private medical records would remain secure even if the email fell into the wrong hands.

Development of the Data Model

- The workgroup developed a data model to support the querying of provider directories to discover electronic service information. Click here to review the data model.
- The data model is standards agnostic and extensible to other standards.
- The workgroup aligned the data model to LDAP/HPD and X12N 274, three electronic data interchange standards popular in the health care community.

Data Model Overview

The Electronic Service Information Discovery Data Model includes the following components:

1. Object Data Set - data elements and definitions for all data objects
2. Query Data Set - data elements for query transactions
3. Response Data Set - data elements for response transactions
4. Data model assumptions
5. Query and Response Descriptions and Examples - detailed overview of valid query and response transactions

X12N 274 and LDAP/HPD Standard Mapping

- The Use Case 2 workgroup mapped the data model to two popular electronic data interchange standards
- The mappings are meant to provide illustrative examples to those that implement the data model. Click here to review the mappings.

Next Steps

- The Electronic Service Information Discovery workgroup will present their work to the HIT Standards Committee (HITSC) for approval.
- Pending HITSC approval, the ONC will pilot and test the technical findings of the workgroup.
- Finally, the data model and data mappings will be released to the public for testing, review, and use.

The Office of the National Coordinator for Health Information Technology

For more information on the S&I Framework, please visit:

http://wiki.siframework.org