IIS and HIE:
Web Services Strategies

March 2014 (v3)

HLN Consulting, LLC®
info@hln.com
http://www.hln.com/

Table of Contents

The purpose of this paper is to describe the options that are available to immunization information system (IIS) projects in collaborating with health information exchanges (HIE) or other service providers to facilitate the exchange of immunization information between electronic health record systems and IIS. In many jurisdictions HIEs can play an active role in providing part of the technical infrastructure to make EHR-IIS interoperability work, especially through the use of SOAP-based web services, the current interoperability transport standard for these transactions. Various options are available for deployment of these web services with differing operational and security implications for both the HIE and IIS projects.

1   Introduction

Immunization Information System (IIS) projects are increasingly becoming interoperability projects. The desire to collect a consolidated record of a patient's immunizations from all sources has always been a primary functional imperative for IIS; these functions support many activities including clinical decision support (CDS), reminder/recall for due or overdue vaccines, vaccine inventory management and eligibility for special programs like Vaccines for Children (VFC), and practice-level assessment. The advent of electronic health records – and the pressure on the entire healthcare system to reduce its cost and increase its efficiency – has led to the development of electronic health record systems (EHR-S). The CMS EHR Incentive Programs have lit an even stronger fire under both the clinical and vendor communities to develop and implement EHR-S.[1] Providers have always resisted "double data entry" – keying immunization data into *both* local systems *and* centralized IIS. The more local systems that pop up, the less providers want to use the web-based IIS client. So the activity switches to interoperability – harvesting records from EHR-S to populate IIS databases and return complete immunization histories and forecasts back to providers.

Health Information Exchanges (HIEs) are collaborative efforts that focus on sharing health data in a community, county, or even on a state-wide basis. They can provide new and efficient ways for public health agencies (PHAs) and IIS projects to receive and send data, especially from the clinical community. The purpose of this paper is to describe the options that are available to immunization information system (IIS) projects in collaborating with health information exchanges (HIE) or other service providers to facilitate the exchange of immunization information between electronic health record systems and IIS. More specifically, this paper discusses different options for the deployment of SOAP-based web services to support both data submission to an IIS as well as data query and response. Some of the material in this paper may seem overly technical to some readers, and it is not the intention of the authors to provide a complete description or tutorial in the underlying technologies being discussed. Additional information can be found in various sources footnoted throughout.

---

[1] http://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html

2   Immunization Information Systems

Nearly every US state and territory has an IIS, defined by the Centers for Disease Control and Prevention (CDC) as, "…confidential, population-based, computerized databases that record all immunization doses administered by participating providers to persons residing within a given geopolitical area."[2] IIS have been around for nearly twenty years. The vision for the IIS of the future is one centered around interoperability: the requirements for IIS to interoperate with other IIS across the country as well as other public health programs within an agency[3] will continue to grow.

For providers, access to IIS has always been a key objective to support clinical care, support quality measures, and provide coverage information required by public health agencies to perform their population-level monitoring and assurance functions. Providers access IIS directly through web-based clients, but increasingly they access indirectly through local EHR systems (EHR-S). The CMS EHR Incentive Programs have accelerated the deployment of EHR systems and promoted standards-based interoperability via HL7 messaging.

3   Health Information Exchange

One of the challenges with interoperability is providing robust, reliable, and cost effective connections between practice sites and IIS, and HIE supports these new ways of sharing data. HIEs are collaborative efforts that focus on health data exchange in a community, county, or even on a state-wide basis (Figure 1)**.** They have a wide and varied set of participants (providers, labs, hospitals, health plans, public health agencies, pharmacies, and patients/citizens). Note that the term "HIE" can be used as both a *verb* and a *noun*: As a verb, HIE refers to the *act* of exchanging data through whatever means and using whatever technology that is selected. As a noun, HIE refers to the physical network or organization that enables the data exchange to take place (sometimes the organizations are call Health Information Organizations, or HIOs).

While compatibility with *de facto* or emerging standards by systems which exchange data is important, HIEs are in a good position to provide the necessary gateways and translations for their members, including public health agencies (PHA), where their systems may be less capable of supporting standards-based interoperability. Many states are also focusing their connectivity options through a single state gateway or portal, providing leveraged connections for simpler, less costly, and less redundant data exchange**.**

---

[2] http://www.cdc.gov/vaccines/programs/iis/about.html
[3] For a more thorough discussion of this notion see Arzt, Noam H., *Evolution of Public Health Information Systems: Enterprise-wide Approaches,* July 2007. <https://www.hln.com/assets/pdf/UT-White-Paper-Final.pdf>
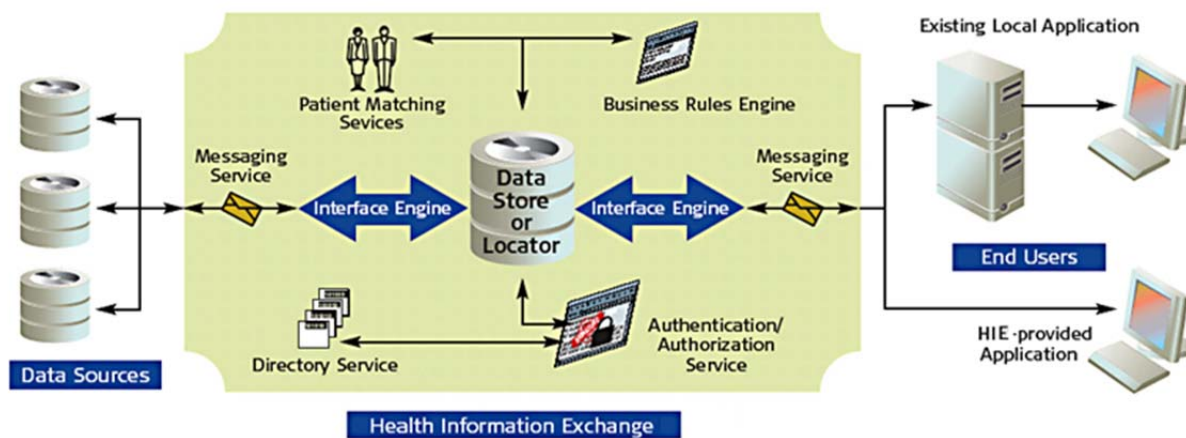
Figure 1

4   IIS Interoperability and Web Services Integration

It is important that both parties participating in an interoperability transaction agree on the means that will be used to transport data reliably and securely. Systems that implement a service-oriented architecture[4] often use Simple Object Access Protocol, or SOAP, as the transport mechanism. This paper is not intended as either a tutorial in basic web services theory, design or development, nor as a configuration guide for any particular implementation. In January 2011 the CDC convened an expert panel to evaluate transport layer strategies for EHR-IIS communications.[5] After considering several alternatives carefully, the panel chose SOAP-based web services as the recommended standard. Additional resources were subsequently developed to assist in implementation, including a standard Web Services Definition Language (WSDL) file.

This emerging national strategy would best be supported by IIS projects implementing fairly uniform, compliant web services to allow EHR system vendors to implement *one* interface for their products that can be used with multiple IIS. Initially, however, some IIS deployed SOAP-based web services using local configurations in the absence of a national standard. An older WSDL may become increasingly difficult to implement and support using modern web services tools and may introduce subtle errors that become harder and harder to diagnose and eliminate. Web services problems can manifest in a variety of locations within the architecture, including the outbound firewall, inbound firewall, networks (DNS, routing, connectivity), SSL/TLS negotiation for encryption, WSDL/web service incompatibility, and even within the HL7 payload. Debugging web service problems requires technical staff on both the sending and receiving ends and is best done with access to logs (*e.g.,* web server, web service, HL7 parser) and raw messages from both ends of a transaction. This type of access may require additional system privileges on one or more of the servers involved. SOAP-based web services, as well as

---

[4] http://www.hln.com/assets/pdf/soa_final.pdf
[5] http://www.cdc.gov/vaccines/programs/iis/interop-proj/ehr.html#technical

the underlying network (TCP/IP) and encryption (HTTP over SSL/TLS) technologies, are mature and well-understood with good debugging tools and wide support. It is essential, however, that implementations use up-to-date versions of the web services specifications (*e.g.,* WS-I Basic Profile 1.1+ which is typically either ASP.NET 2.0+ or JAX-WS 2.0+).

It is also important that a project define clearly its web services support strategy, especially when a partner organization (*e.g.,* an HIE) is providing some of the web services infrastructure. Some of the options described below involve multiple web services; the "handoff" of data between these services should be as transparent as possible to the data partner, and the support program put in place should minimize "finger pointing" between service providers (*e.g.,* the IIS and the HIE). Support services may need to go beyond simply giving data partners access to documentation, though that may be sufficient for experienced users or stable, more standard web services. Many data partners will require some share of "hand-holding" to help figure out connectivity problems or examine payload messages to fix incompatibilities, especially when data partners are less experienced or less motivated, or web services are less standard. A single entity should take responsibility for the entire architecture from a support standpoint and have access to all service logs and messages between participants, as well as provide coordination between the data sender (typically the provider) and recipient (typically the IIS) and all the intermediary points along the way (*e.g.,* an HIE). In many settings this may be difficult to achieve because of the reality of the politics within a particular region. IIS projects may be in the best position to provide this leadership when there are no intermediaries active or where immunization transactions are the primary data exchange activity taking place; HIEs may be in a better position in more sophisticated regions where many different HIE transactions are taking place.

5   Web Services Options

A variety of options for web services deployment are available to an IIS (Figure 2). These options differ in not only their technical configurations but also in their support services requirements since some of these options are deployed cooperatively by the IIS and a partner organization which may be an HIE or even a larger jurisdictional information technology support agency which may control the exposure of services to the Internet. For the balance of this discussion we will refer to all such external partner organizations as "HIEs" regardless of their actual name or function, since we assume they are functioning in a similar capacity.

Less Sophisticated   *More Sophisticated*

Direct
(IIS WS addressed with no HIE involvement)

Pass-through
(HIE passes WS calls to IIS and back)

Intermediated
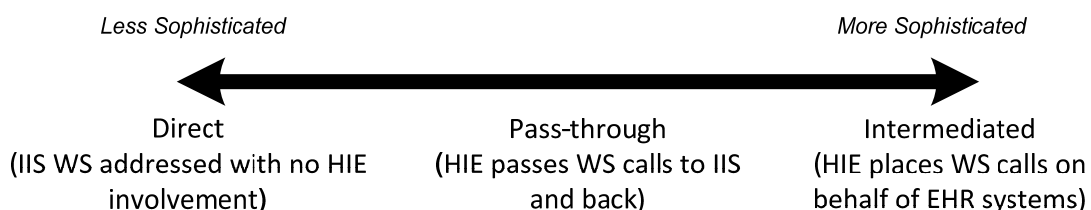(HIE places WS calls on behalf of EHR systems)

Figure 2 – Web Services Integration Options

While it is possible to evolve from one of these options to another, projects should be careful to understand the *client*-side (*i.e.,* the provider-side) implications of changes in strategy: in most cases, changes in web services strategy that would require changes to other parties' implementations should be avoided as it may require extensive testing to assure that interfaces are still functioning as before. It is also possible that some partner organizations will require changes to their vendor-provided solutions *or* deployment of solution components that are *not* able to be provided by their current vendors.

5.1 Direct Web Service

Using this option, the EHR systems (or other clients) address a web service exposed directly by the IIS itself. This style of web service is typically the way most IIS products (commercial or otherwise) are configured to be deployed – the status quo. There is typically no requirement for any other intermediary or organization, such as an HIE, to be involved in the deployment. The IIS team is completely responsible for technical deployment and technical support, including on-boarding of new data partners and configuration of all interfaces. This option is best when there are no intermediaries available (like an HIE), and/or when PHAs have robust support infrastructures available for data sharing partners.

The strengths and challenges of this option include:

Strengths	Challenges
• Quickest to implement. • Usually involves the fewest steps to implement. • Involves the fewest organizations. • Requires no additional cost beyond the capabilities of the IIS.	• Does not leverage HIE infrastructure, relationships, or organization. • IIS may have insufficient level of staffing to configure, test, and maintain the required number of interfaces.

5.2 HIE Pass-through

Using this option, the IIS partners with another organization, typically an HIE, to provide the exposed URL for the IIS web service through one of several sub-options which will be described below (Figure 3).
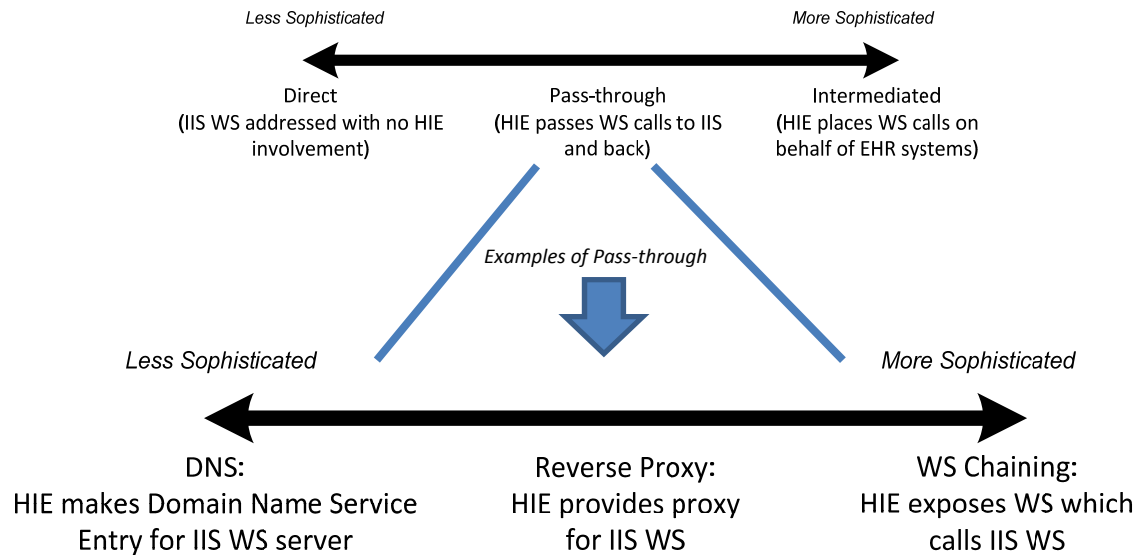
Figure 3 – Web Services Integration Pass-through Options

In all cases for these sub-options, the URL exposed to the data partners appears as an HIE URL rather than an IIS URL. This option is best when there is a desire to focus the visibility of the data exchange transaction to the HIE for legal, political, or support-capability purposes. In some jurisdictions, public health data submissions are required to pass through a state-level HIE by law or policy. The pass-through option provides the simplest way to achieve this outcome. In some cases, this "branding" may or may not be consistent with the desires of either the IIS or HIE projects.

5.2.1 Domain Name Service (DNS) Sub-option

For this configuration to work several steps are required:

1. The IIS and HIE select a hostname with the namespace of the *HIE* (*e.g.,* iis.state-hie.org). The Internet Service Provider (ISP) of the HIE points that name to an IP address belonging to the IIS web service host.
2. The IIS creates a virtual host in its web server configuration so that the web server knows how to properly respond to requests made to the new hostname (in this example, iis.state-hie.org).
3. The HIE *or* the IIS acquires an SSL certificate for the new hostname to ensure that encryption can be enabled.
4. The IIS installs the SSL certificate on its server.

Note that though the HIE is selecting a hostname, it is not actually hosting any IIS services at all. It is simply allowing its ISP to route traffic for that hostname to the IP address provided by the IIS.

The strengths and challenges of this sub-option include:

Strengths	Challenges
• Minimal additional effort for both the IIS and HIE to configure and deploy. • Brings the HIE into the project as the web services are "branded" with the HIEs domain. • Minimal additional cost to configure and deploy. • No actual data passes through the HIE, so no additional security exposure is introduced.	• Requires HIE-IIS technical cooperation to setup/maintain. • Minimal leverage of HIE infrastructure, relationships, or organization. • No change in the level of IIS staffing to configure, test, and maintain the required number of interfaces.

5.2.2 Reverse Proxy Sub-option

For this configuration to work several steps are required:

1. The HIE exposes a true web services URL within its address space (*e.g.,* https://iis.state-hie.org/IISWebService).
2. The HIE web server is configured to proxy this to an IIS URL which is the actual web service. As calls are made to the HIEs web service they are transferred by the HIE to the actual IIS web service through the proxy.
3. The HIE installs and configures an SSL certificate on its web server to ensure that encryption can be enabled.

Note that in this case data is passing through the HIE but the HIE should not be capturing any data nor providing any actual services other than the proxy.

The strengths and challenges of this sub-option include:

Strengths	Challenges
• Brings the HIE into the project as the web services are "branded" with the HIEs domain. • Minimal additional effort for the HIE to configure and deploy. • Even less technical cooperation necessary between the IIS and HIE than DNS sub-option.	• Operation of the service dependent on the HIEs successful maintenance of the reverse proxy. • Minimal leverage of HIE infrastructure, relationships, or organization. • Data passes through the HIE, so an additional security exposure is introduced. • No change in the level of IIS staffing to configure, test, and maintain the required number of interfaces.

5.2.3 Web Services Chaining Sub-option

For this configuration to work several steps are required:

1. The IIS and HIE select a hostname with the namespace of the *HIE* (*e.g.,* iis.state-hie.org).
2. The hostname resolves to an HIE server which hosts one or more web services addressable by the external data partner systems (*e.g.,* EHR systems).
3. HIE acquires and installs an SSL certificate for the new host to ensure that encryption can be enabled.
4. The HIE web services call the corresponding IIS web services and pass the result of the transactions back to originating entity.

Note that in this case data is passing through the HIE but the HIE should not be capturing any data nor providing any actual services other than the proxy.

The strengths and challenges of this sub-option include:

Strengths	Challenges
• Brings the HIE into the project as the web services are "branded" with the HIEs domain. • Moderate leverage HIE infrastructure, relationships, or organization. • Even less technical cooperation necessary between the IIS and HIE than DNS sub-option. • Data passes through the HIE creating an opportunity for value-added services.	• Operation of the service dependent on the HIEs successful maintenance of its web services. • Requires more infrastructure and configuration by the HIE. • Data passes through the HIE, so an additional security exposure is introduced. • No change in the level of IIS staffing to configure, test, and maintain the required number of interfaces. • Technical support now requires close cooperation between IIS and HIE to debug and fix problems. • Web services proxy increases complexity as well as the number of places where a problem can occur (*e.g.,* now there are *two* outbound and inbound firewalls, *two* web services, *two* SSL/TLS sessions to negotiate, etc.).

5.3 HIE Intermediation

Using this option, the HIE itself is the entity which is making web services calls to the IIS on behalf of other systems to which it is connected, typically the EHR systems of its member organizations. No changes are required to the web services offered by the IIS which operate as

Direct Web Services similar to those in the first option above. This option is best when the HIE is providing value-added services (like data aggregation on behalf of its members across various data sources) or when the HIE is cooperatively involved in on-boarding providers and supporting provider interfaces to the IIS through the HIE. Keep in mind, however, that debugging of technical problems and technical support in general is now much more complex: the technical staffs of both the HIE and IIS project need to work very closely to ensure that end-to-end connectivity is successfully and consistently achieved without "finger pointing" visible to the data sharing partner.

The strengths and challenges of this sub-option include:

Strengths	Challenges
• Significant leverage HIE infrastructure, relationships, or organization. • Data passes through the HIE creating an opportunity for value-added services. • HIE maintains more control over the query and can manipulate, if desired, both the query and the response. • Significant technical cooperation may be necessary between the IIS and HIE. • Larger burden of the provider-IIS interface is placed on the HIE and its existing connections to the provider, easing some project-specific challenges. • IIS should require significantly lower level of staffing to configure, test, and maintain the required number of interfaces.	• Requires significant trust by the IIS that the HIE will query and handle the result properly. • Requires more infrastructure and configuration by the HIE. • Data passes through the HIE, so an additional security exposure is introduced. • Technical support now requires close cooperation between IIS and HIE to debug and fix problems. • IIS may lose the ability to send web services acknowledgements, errors, or responses directly to the data partner.

6 Conclusions

IIS and HIE projects need to work together to determine which option is best. In large part, choices will depend on how stakeholders wish for the HIE to be involved in IIS data exchange – both short-term and long-term. While the first option – direct web services access – represents the simplest, status quo choice, it may become increasingly difficult for the IIS project to support alone as it scales to a larger and larger number of data partners, and may over time appear as an "outsider" if more and more interfaces begin to move through an HIE. The HIE pass-through options may appear primarily as "cosmetic" solutions to get an HIE more conspicuously involved in IIS data exchange, but one or more of the sub-options may represent a stepping stone, or incremental step, towards fuller HIE intermediation. Projects should consider HIE intermediation within the context of overall long-term HIE/public health data exchange strategy. An IIS with a legacy WSDL (*i.e.,* not using the CDC standard WSDL) may benefit from partnership with an HIE which can deploy the standard WSDL and improve the quality and compatibility of provider interfaces with little to no additional work by the IIS.