Oregon ALERT IIS

Real Time Data Exchange
For HL7 Messaging

Version 3.0
Last Updated: September 10, 2018

Contents

Introduction

Thank you for your interest in electronic data exchange with Oregon ALERT IIS.

Data is exchanged in real-time, with Oregon ALERT IIS, using HL7 version 2.5.1 through SOAP[1]-based web services. These services include methods for submission of immunization data and querying of patient history and forecast. Reference the CDC[2] HL7[3] Version 2.5.1: Implementation Guide for Immunization Messaging, Release 1.5[4] for message format and content requirements.

Onboarding for new client connections to the ALERT IIS web service requires an approval process consisting of planning, development, and testing phases. The ALERT IIS Program makes every effort to expedite these phases, but the length of time required may vary widely, depending on a multitude of factors.

Direct questions or requests for further information to the **ALERT IIS Help Desk** and ask for a Data Exchange Analyst: **1-800-980-9431** or alertiis@state.or.us.

[1] Simple Object Access Protocol
[2] Centers for Disease Control and Prevention
[3] Health Level Seven (visit http://www.hl7.org for details)
[4] https://www.cdc.gov/vaccines/programs/iis/technical-guidance/hl7.html

Process Summary

The following list provides a quick, at-a-glance summary of the usual steps which are involved in connecting to the ALERT IIS data exchange services for the first time.

Gather Information

Before proceeding with other steps, it is important to have all necessary information confirmed and available. Most of the information needed will be in relation to your Electronic Health Records (EHR) system – e.g., software vendor, version, pertinent modifications, other important technical implementation details. It is also advisable to review relevant documentation regarding HL7 and electronic data exchange – the CDC HL7 2.5.1 Implementation Guide[5] is a great place to start with this review.

Contact ALERT IIS Program

Get in touch with ALERT IIS Program staff to discuss your intention to access the ALERT IIS using real-time data exchange processes. This contact will initiate the process and move it along to the next steps, including permissions & set-up for using the ALERT IIS testing environment.

Plan & Develop Solution

Depending upon details related to your EHR system, and other variables, a technical solution for making web service requests to the ALERT IIS will need to be developed. In some cases, this solution may be as simple as making configuration changes to existing functionality already available within the client EHR system. In other cases it may involve some level of custom development work, or more technical configuration changes. In either case, it is likely that the solution will be coordinated with whatever technical staffing resources are used to manage the client EHR system.

Perform Tests & Obtain Approval

All new connections to the ALERT IIS must be validated in the test environment before moving to the active, production environment. Both environments require data exchange requests to be authenticated with a username/password combination. Authentication credentials for the test environment are acquired first, after which the testing phase proceeds for as long as is necessary to confirm that messages are being sent correctly.

Begin Data Exchange in Production Environment

After test confirmation, new authentication credentials for the production environment are provided to the client, at which point real time data exchange may commence.

[5] https://www.cdc.gov/vaccines/programs/iis/technical-guidance/hl7.html

General Concepts

You may wish to skip this section if you already have a working technical understanding of web services.

Web services are means for one computer to access functions in another computer not located on the same L/WAN[6]. In most cases the two hosts communicate with one-another across the Internet. Communication between hosts is established, handled, and secured in fundamentally the same way that a human user accesses a website, through a web browser. The term "web service" is actually a broad term which may reference one of several different means for host-to-host communications using HTTP/S.

Transport & Security

Web communications typically use a protocol known as HTTP[7], or its variant HTTPS[8]. When using HTTPS, communications are said to be trusted, and are secured using encryption. Trust and encryption are accomplished by means of an additional protocol known as SSL[9] or TLS[10]. In this trust relationship, a client requests that a server identify itself[11] using a certificate with verifiable validity.

The client also asks that communications be encrypted using one of several possible cipher suites – a set of algorithms which designate how messages will be encrypted and decrypted. Available cipher suites change over time, with some suites becoming less or more favorable, depending on a number of factors. In some cases, older cipher suites are deprecated altogether and dropped from use.

Web Service Requests

In much the same way that one navigates to a website using an address (i.e., URL[12]), web services requests are also made by specifying the URL at which the server hosts the web services. The web service URL is referred-to as an "end point."

Oregon ALERT IIS web services are accessed using SOAP. If you consider website content (i.e., HTML[13]) as the information transmitted within an HTTP/S communication, then a SOAP message is simply a different sort of content, intended for interpretation by methods on each host, rather than inside a web browser. SOAP-based web service communications must be handled in precise ways, as defined in a special file presented in WSDL[14] form.

A WSDL file is made available by a server which offers web services for consumption[15]. The WSDL file tells the client what methods[16] are available, exactly how to access those methods, and what to expect, in response.

---

[6] Local/Wide Area Network
[7] Hypertext Transfer Protocol
[8] HTTP Secure
[9] Secure Sockets Layer
[10] Transport Layer Security
[11] Note that prior to February of 2018, Oregon ALERT IIS required clients to identify themselves with certificates. This requirement has been changed such that clients no longer need to present certificates.
[12] Uniform Resource Locator
[13] Hypertext Markup Language
[14] Web Services Description Language
[15] Clients which access web services from a server are often said to "consume" those services.
[16] A web service "method" is a generic term for a specific task which a client may ask the server to perform.

Implementation

Refer to the Onboarding Checklist section for a step-by-step outline of the entire implementation process.

The most common implementation for access to the Oregon ALERT IIS web service is through configuration of a client EHR[17] system.

Hosting Environments

In addition to the main, production hosting environment, Oregon ALERT IIS also maintains a wholly separate hosting environment for testing. The test environment is used for set-up and confirmation of new or changed client configurations. All configurations must be confirmed against the test environment before being approved for the production environment.

WSDL Files

Oregon ALERT IIS web services implement the WSDL file promulgated by the CDC for standardization of IIS web service communications. This is known as the "common" WSDL file for IIS data exchange and is recommended for use by all web service clients[18].

In addition to the common WSDL file, however, Oregon ALERT IIS also implements its own, "local" file, which was generated prior to the existence of the common WSDL file. For the sake of continuity and compatibility, the local file is still valid for use.

Additional information for retrieval of the actual files is contained in the following section.

Service End Points

Client EHR software should be configured to connect to a specific web service "end point" according to which WSDL file they implement, and which hosting environment is to be accessed.

Hosting Environment		
Testing	CommonWsdl	`https://soa.alertiis.org/cdc-trn-webservices/client_Service?wsdl`
	Endpoint	`https://soa.alertiis.org/cdc-trn-webservices/client_Service`
Production	CommonWsdl	`https://soa.alertiis.org/cdc-prd-webservices/client_Service?wsdl`
	Endpoint	`https://soa.alertiis.org/cdc-prd-webservices/client_Service`

Table 1. Oregon ALERT IIS web service end-points

Specific WSDL files, for each separate end point, may be obtained by simply adding a query directive for "wsdl" to the end of each URL, for example:

`https://soa.alertiis.org/cdc-prd-webservices/client_Service?wsdl`

Connecting

Client connections must also be configured to authenticate with a valid username and password pair. These authentication credentials may be obtained by working directly with ALERT IIS Program staff, during the onboarding process.

[17] Electronic Health Records

[18] Visit the CDC website at https://www.cdc.gov/vaccines/programs/iis/technical-guidance/soap/services.html for more details.

Sending Requests

Requests are sent to the Oregon ALERT IIS web services host by means of HL7 data contained within SOAP messages. Requests are always for one of two different types of possible action:

1. A query to retrieve resulting, return data, for immunization histories
2. Transmission of new or updated information regarding vaccines administered

Web services provide named "methods" for processing requests. The client indicates, in the request, which of the named methods are to be accessed. For the two possible WSDL files available for the Oregon ALERT IIS web services, the method naming, and mode of access differs.

If using the CDC's common WSDL file, each of the two possible types of request are accessed by referring to one method, named **submitSingleMessage**.

For the local WSDL file, a separate method is made available for each of the two types of operation. For queries, the method name is **FindHistory**; for updates, **UpdateHistory**.

In either case, the SOAP message sent as the request will contain an HL7 message segment. In the case of the common WSDL file, the nature of the request is determined by whether the header (MSH) portion of the HL7 message segment indicates a VXU[19] or QBP[20] type. The HL7 message segment contains the data necessary to perform the desired update or query operation.

For the common WSDL file, only, there is another operation available for simply testing connectivity parameters, without making an actual request for a specific action. The method for this operation is named **connectivityTest**.

Responses & Faults

If a successful connection to the Oregon ALERT IIS web service host is made, the client may expect a response which indicates a completion status, and return data, if a query operation was requested. It is up to each individual implementation (whether through an EHR system or other means) to process these responses.

Of particular importance are responses which indicate that the server encountered some manner of fault while attempting to process the incoming SOAP request message. There are three types of specific, known fault types which may be generated:

1. **Unsupported Operation**: the incoming request specified an operation (method type) which is not defined as part of the ALERT IIS – i.e., anything other than the named methods defined within each WSDL file.
2. **Security**: each request to the server must be authenticated using security credentials (username and password pair). A security fault is returned if authentication fails.
3. **Message Too Large**: the HL7 component of the request is longer than the maximum length allowed (as specified within the WSDL file).

[19] Vaccination Record Update (VXU-V04)
[20] Request Immunization History (QBP-Q11)

In addition to these specific problems, if any other sort of SOAP fault is encountered during processing of the incoming request, the server will reply with an **Unknown** fault message.

Troubleshooting

For problems which occur at the stage of processing successfully received requests, troubleshooting should be relatively straight-forward. The receipt of a SOAP fault message, returned from the server, will serve to eliminate connection problem as the fundamental issue, and provide useful insight into the nature of the problem. Typically, these problems will involve simple changes to values being sent by the client, within the request message.

Other problems, however, may arise, wherein no fault message is returned, or the reply message contains unexpected contents. In these cases, one of the following two types of issue is likely being encountered:

Connectivity or Communication Problems

As outlined in the foregoing sections, there are several factors involved in establishing network connectivity between clients and the Oregon ALERT IIS web service host. These factors include proper routing of TCP/IP communications and security/encryption protocols. The request-sending client must have a clear channel for communication with the web service host – meaning that network perimeter security measures must allow for the passage of outgoing and incoming communications. Network routing and firewall set-up rules will cause connections to fail if outgoing requests or incoming responses are stopped.

It is also possible that problems which arise anywhere along the communications pathway – within the client or ALERT IIS LAN/WAN environment, or along the Internet pathway in-between – may temporarily prevent successful processing of requests.

Internal Processing Problems

Though generally less likely than other issues, it is possible that bugs in either the client system or the ALERT IIS may interrupt normal processing of web service requests. A bug in the client system, for example, may occur while formulating a request, and thus the request never is sent, without any indication that the send request never occurred. Similarly, a bug in the ALERT IIS may prevent the processing of a properly-formed request, in which case it is possible that no response is ever sent – including a fault message. Such a circumstance would be exceedingly rare, however, and should always be an outlying consideration when attempting to troubleshoot issues.

Onboarding Checklist

The following outline may be used as a checklist to guide oneself through the process of real-time data exchange onboarding with the Oregon ALERT IIS:

1) Planning & Design

- ☐ Review the CDC HL7 2.5.1 Implementation Guide for HL7 messaging specifications. Please note Oregon-specific HL7 requirements:
    - Clinic level code (AL#, provided by ALERT) must be sent in MSH-4. It can instead be sent in MSH-22 if MSH-4 identifies the sending application.
    - Clinics participating in the Vaccines for Children program must send Oregon specific vaccine eligibility codes for all administered doses for all patients.
- ☐ Write a test plan and set up test cases/patients in your test environment.

2) Development

For EHR products that have received 2014 or 2015 ONC-ATB certification:

- ☐ Verify that VXU and QBP messages meet the CDC HL7 2.5.1. specifications and passes the NIST certification tests.
- ☐ Confirm that the clinic(s) onboarding for data exchange are on the correct EHR version (see step above) to ensure that messaging meets minimum standards.

For EHR products not certified for Meaningful Use:

- ☐ Develop VXU and QBP messages that meet the CDC HL7 2.5.1. specifications and pass the NIST certification tests.

For all EHR products:

- ☐ Configure interface to ALERT IIS-specific requirements:

    For EHRs supporting query messaging, consider the following questions as part of planning and development:

    - Will patient histories returned by ALERT IIS be incorporated in the patient's history in the EHR? Will deduplication of data happen automatically and manually be end user?
    - Will the EHR automatically trigger a query for patient history based on appointment check-in or scheduling? Or will the clinic user initiate the query manually from the interface?
    - How will the returned records be displayed to the user?

- Error Message and Response File Management. Please consider the following questions in your planning and development:
    - Who will review and resolve interface errors, data and connectivity?
        - If there is web service downtime for maintenance or outage, what is the plan for how records will be re-sent?
    - How will the EHR manage HL7 acknowledgement messages?

- How will errors be presented to the clinic or end user?
- How will providers be able to correct errors and re-submit?

3) Onboarding Call with ALERT IIS Data Exchange Team

☐ Confirm with ALERT IIS that sites have an established site agreement with ALERT IIS. Add/modify as needed.

☐ The purpose of this call is to review design and development steps, determine readiness and review next steps for testing and deployment. Please contact the ALERT IIS Help Desk: alertiis@state.or.us

4) Webservice Configuration

☐ Configure interface engine or EHR for the test environment, see detail in the Implementation section of this guide

- Obtain username/password with ALERT IIS data exchange analyst
- Use of the Common WSDL is recommended
- Choose appropriate webservice endpoint
- Prepare to independently research/troubleshoot connection issues

5) Testing

☐ Confirming Message Format

- Submit single messages reviewing acknowledgement messages and correcting format as needed.
- Conduct internal QA and validation of test messages.

☐ Confirming Message Content

- Submit live data to the ALERT IIS test region in realtime
- Compare results to existing production region submission and/or obtain confirmation from the site that data submitted is complete and accurate.

6) Review results of testing with ALERT IIS Data Exchange Coordinator. Conduct additional testing as requested by Data Exchange Coordinator. Once interface is approved by Data Exchange Coordinator, schedule Go-Live.

7) Deployment

☐ Coordinate date for go-live with ALERT IIS Data Exchange Coordinator. Manual entry in to the ALERT IIS website or manual uploads to the IIS should not be eliminated until HL7 realtime exchange is established.

☐ Validate data going to ALERT IIS production and review with ALERT IIS Data Exchange Coordinator.

☐ Establish ongoing data monitoring practices in clinics by using ALERT IIS reports to assure that data being reported is complete and accurate.