OneHealthPort HIE

Connectivity Implementation Guide

Washington Immunization Information System (WAIIS)

Revised: **February 2020** Version **1.0**

Table of Contents

1. DOCUMENT CHANGE HISTORY

DOCUMENT NAME: Implementation Guide – WAIIS			
Version	**Issue Date**	**Modified By**	**Comments/Reason**
1.0	3/11/2019	Rhonda May	First draft of WAIIS IG
1.0	4/2/2019	Kelly Llewellyn	Editing contributions for formatting; clarifications for SOAP envelope
1.0	5/3/2019	Kelly Llewellyn	Edits incorporated from Washington State Department of Health WAIIS team
1.0	2/3/2020	Deb Wilson	Clarify Timestamp Signature Requirement. Add Transaction Testing Checklist.

2. INTRODUCTION

2.1. Overview

The Washington State Department of Health (DOH) operates the Washington Immunization Information System (WAIIS), which includes reported information on immunizations administered in the lifetime of Washington residents. Information in the registry is available to all licensed healthcare providers in Washington to support immunization activities.

The OneHealthPort Health Information Exchange (OHP HIE) supports synchronous (web service) and asynchronous (AS2) access to WAIIS for purposes of reporting immunization information as well as queries for information from the registry.

The OHP HIE will programmatically prepare messages for delivery to WAIIS. Acknowledgements and Responses from WAIIS will be delivered back to the submitting organization.

2.2. Scope

This implementation guide defines the **connectivity requirements** for immunization reporting and query/response transactions to/from WAIIS.

The detailed onboarding guide and transaction content for WAIIS is available on the DOH website as a (PDF) document. WAIIS HL7 Interface Project Guide.

This transaction is for licensed healthcare providers with an active OHP HIE contract agreement, submitting immunization administration information and accessing patient immunization history from WAIIS via the OneHealthPort HIE. This guide is unique to ***One*HealthPort.**

2.3. Terms and Acronyms

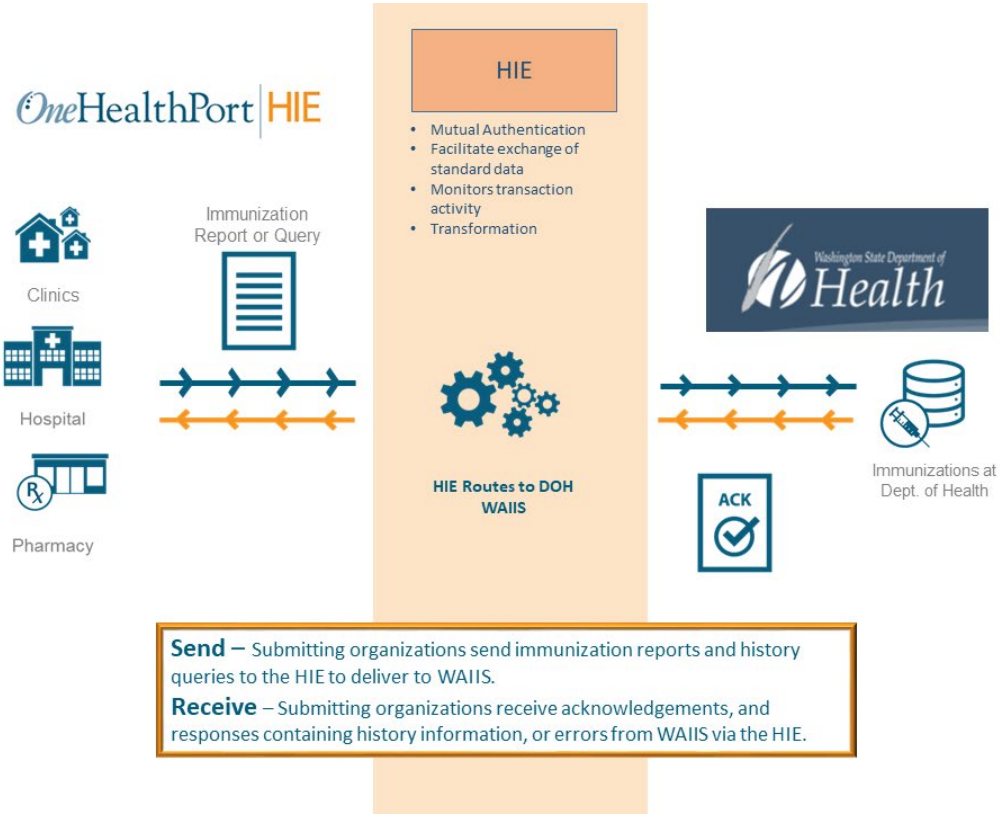
Term/Acronym	Description
WAIIS	Washington Immunization Information System
HIE	Health information exchange
DOH	State of Washington Department of Health
OHP	Refers to OneHealthPort
CA	Certificate Authority

2.4. Assumptions

- Organizations submitting immunization reports and performing queries for immunization history from WAIIS are registered to do so with the DOH.
- All transactions between the HIE and requesting systems will utilize one of the following connectivity methods:
    - The Activator or an approved AS2 connection for the secure transport of the transactions both in and outbound (asynchronous transaction).
    - A web service connection through appropriate certificate exchange and message encryption (synchronous transaction).
- In response to immunization reporting and immunization history queries to WAIIS, acknowledgements/responses returned will be transferred to the submitting organization.
    - Web service processing will return responses to the submitting organization synchronously.
    - Submitting organizations using the Activator connectivity software or an approved AS2 connection will access and move the responses through their Activators or AS2 tools asynchronously.
- Immunization message content validation and support for report, query, acknowledgements and responses are handled by the WAIIS onboarding team directly with the submitting organization and their vendor.

3. PROCESS FLOW

3.1 High Level Process Flow Diagram



The OHP HIE is a secure intermediary between requesting practices, hospitals, pharmacies or other licensed healthcare professionals reporting or requesting patient immunization information from the WAIIS. The WAIIS houses all data and authenticates all requests by checking user name and password to ascertain that the identifier of the requestor is associated with an active account.

4. WEB SERVICES TRANSACTION REQUIREMENTS

4.1 Certificate Requirements

The OneHealthPort HIE web services use the open internet to allow maximum bandwidth for message exchange. Certificate Authority issued certificates are used to sign and encrypt the messages using full Public Key Infrastructure (PKI) sent via a secured channel (https).

Organizations choosing web services are required to provide certificates to the OneHealthPort HIE. Only certificates from a third-party certificate authority are accepted for use. The same CA issued certificate may be used with both the production and UAT (test) environments. In addition, if a trading partner has already exchanged certificate information for other OneHealthPort web service transactions, that same certificate can be used for WAIIS transaction processing.

Certificate requirement details:

- Certificates supplied must be from a well-known and trusted commercial certificate authority that complies with the CA/Browser Forum standards – self-signed certificates will not be accepted
- The same certificate may be used with the production and UAT (test) environments
- Certificates will use a minimum of a 2048-bit key size for RSA (4096 is preferred) and SHA256 with RSA for signatures.
- Standard or Basic SSL certificate for a single Domain name (Wildcard or multi-domain is not required unless that is your organization's standard)
- Validity option: 1-3 years
- Preferred format - A digital certificate will be required for secure exchange of data. This may be in the form of either a DER encoded binary X.509 (.cer) or Cryptographic Message Syntax Standard PKCS #7 (.p7b, .p7c). If a .p7b/.p7c file is going to be used please export the entire certificate chain for use during the connectivity process
- Provide full certificate chain from a third-party certificate authority PLUS the public key.
    - The submitting organization will sign the WAIIS transactions inbound to the web services gateway with their private key.
    - The submitting organization public key will be used at the web services gateway to decrypt the messages for transformation and forward to WAIIS.

TLS minimum requirements for cipher suite configuration:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA

4.2 Certificate Handling

The certificate generated for trading partner connectivity to the HIE is unique for each partner. The trust relationship is created between each partner and the OneHealthPort HIE through execution of the HIE Participation Agreement.

Each trading partner will only require the certificate of the OneHealthPort HIE to trade with the entire OneHealthPort HIE trading community. The OneHealthPort HIE is designed as a spoke and hub model with a single connection from each participant (trading partner) to the HIE (Hub). Data will flow from the sending party to the HIE and then outbound to the designated receiving party.

All the transactions to OneHealthPort HIE will be done using certificate based Mutual Authentication. Trading Partner and OneHealthPort HIE will need to exchange certificates prior to establishing the secure connection.

From a high-level point of view, the process of authenticating and establishing an encrypted channel using certificate-based mutual authentication involves the following steps:

1. A client requests access to a protected resource/Service.
2. The server presents its certificate to the client.
3. The client verifies the server's certificate.
4. If successful, the client sends its certificate to the server.
5. The server verifies the client's credentials.
6. If successful, the server grants access to the protected resource requested by the client.

4.3 Signature requirements

OneHealthPort will configure **UAT** web services with trading partner signature as optional to facilitate connectivity and testing. Once connected, trading partners will need to provide signatures in their UAT messages. **All submitters must successfully submit web services transactions with signature in UAT before being authorized to send any production submissions.** Production web services are configured with signature required. Production messages without signature will be rejected.

For signatures, trading partners:

- Sign the timestamp in the message header – the security reference section is added to define the digital signature starting with: <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">. The timestamp must occur within the <wsse:Security> tag.
- Use their own private key to sign the timestamp – the encrypted signature is added in the <dsig:SignatureValue> **of the header**
- Include the public key in the messages – included in the <dsig:X509Certificate>

Verification Process		
User Acceptance Testing (UAT)	**Production**	**Description**
Required	Required	Mutual authentication occurs using the root and intermediate certificate information
Required	Required	Certificate validation occurs using the complete certificate chain with leaf
Optional	Required	Signature validation occurs by signing the timestamp in the SOAP message header

Sample signature signing timestamp in SOAP header:

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:urn="urn:cdc:iisb:2011">
        <soap:Header>
                <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
                        <ds:Signature Id="SIG-D8234953C823AFAE2415536312716865"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                                <ds:SignedInfo>
                                        <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                                <ec:InclusiveNamespaces PrefixList="soap urn"
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                        </ds:CanonicalizationMethod>
                                        <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                                        <ds:Reference URI="#TS-D8234953C823AFAE2415536312715641">
```

```
                                        <ds:Transforms>
                                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-
c14n#">
                                                <ec:InclusiveNamespaces PrefixList="wsse soap urn"
xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                                            </ds:Transform>
                                        </ds:Transforms>
                                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                                        <ds:DigestValue>Content Redacted</ds:DigestValue>
                                    </ds:Reference>
                                </ds:SignedInfo>
                                <ds:SignatureValue>Content Redacted</ds:SignatureValue>
                                <ds:KeyInfo Id="KI-D8234953C823AFAE2415536312716723">
                                    <wsse:SecurityTokenReference wsu:Id="STR-D8234953C823AFAE2415536312716744">
                                        <wsse:KeyIdentifier EncodingType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-
open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3">Content Redacted</wsse:KeyIdentifier>
                                    </wsse:SecurityTokenReference>
                                </ds:KeyInfo>
                            </ds:Signature>
                            <wsu:Timestamp wsu:Id="TS-D8234953C823AFAE2415536312715641">
                                <wsu:Created>2019-03-26T20:14:31Z</wsu:Created>
                                <wsu:Expires>2019-03-26T20:15:01Z</wsu:Expires>
                            </wsu:Timestamp>
                        </wsse:Security>
                    </soap:Header>
```

4.4 Endpoints for WAIIS Web Service Transaction

Endpoint URLs are provided by the OneHealthPort for use by the organization when implementing web services to the WAIIS. The WAIIS web service is a POST transaction and uses a SOAP API sending XML over HTTPS.

OneHealthPort HIE UAT (test) Environment:

Endpoint – https://uat-onehealthport-api.axwaycloud.com:8094/doh/phchub/PHC-Hub/soa

Production system endpoint will be provided upon successful completion of testing.

5. Checklist for Preparing Transaction Testing

5.1 Steps to Complete Before Transaction Testing

- ✓ Initial connectivity testing may use test patient data.
- ✓ Ensure Port 8094 is allowing traffic from the proper servers for both testing in UAT and sending transactions in Production.
- ✓ Ensure you have the correct OneHealthPort FacilityID for the message header.
- ✓ Ensure you have the correct WAIIS FacilityID for the message body.
- ✓ Ensure you have the correct user name and password for the message header.
- ✓ Configure the OneHealthPort public certificate to your server trust store.

- ✓ Configure your private client certificate in your server cert store so during the SSL handshake your certificate is presented to OneHealthPort.
- ✓ There are no special or unique file naming conventions associated with the WAIIS transactions required for appropriate message handling.

  For the AS2 Connectivity, whatever naming convention is used by the request submitter will be seen in the response, preceded by "**WAIIS**".

6. TRANSACTION STRUCTURE

6.1 Transaction Structure

Transaction structure is defined in the WAIIS HL7 Interface Project Guide.

7. TRANSACTION TRANSPORT SAMPLES

The following samples are not to be used as sample code. Message header and body will reflect the development tools capabilities, organization identifiers, and test patient data specific to your organization.

7.1. Request Body– xml Sample (Includes transport header and body)

```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope" xmlns:urn="urn:cdc:iisb:2011">
    <soap:Header>
        <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">
            <ds:Signature Id="SIG-D8234953C823AFAE2415536312716865" xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                <ds:SignedInfo>
                    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                        <ec:InclusiveNamespaces PrefixList="soap urn" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                    </ds:CanonicalizationMethod>
                    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
                    <ds:Reference URI="#TS-D8234953C823AFAE2415536312715641">
                        <ds:Transforms>
                            <ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#">
                                <ec:InclusiveNamespaces PrefixList="wsse soap urn" xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#"/>
                            </ds:Transform>
                        </ds:Transforms>
                        <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
                        <ds:DigestValue>Content Redacted</ds:DigestValue>
                    </ds:Reference>
                </ds:SignedInfo>
                <ds:SignatureValue>Content Redacted</ds:SignatureValue>
                <ds:KeyInfo Id="KI-D8234953C823AFAE2415536312716723">
                    <wsse:SecurityTokenReference wsu:Id="STR-D8234953C823AFAE2415536312716744">
                        <wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0#X509v3">Content Redacted</wsse:KeyIdentifier>
                    </wsse:SecurityTokenReference>
```

```
                    </ds:KeyInfo>
                </ds:Signature>
                <wsu:Timestamp wsu:Id="TS-D8234953C823AFAE2415536312715641">
                    <wsu:Created>2019-03-26T20:14:31Z</wsu:Created>
                    <wsu:Expires>2019-03-26T20:15:01Z</wsu:Expires>
                </wsu:Timestamp>
            </wsse:Security>
        </soap:Header>
        <soap:Body>
            <urn:submitSingleMessage>
                <urn:username>Content Redacted – User name provided by DOH</urn:username>
                <urn:password>Content Redacted – Password provided by DOH</urn:password>
                <urn:facilityID>Content Redacted – Facility ID provided by OHP</urn:facilityID>
                <urn:hl7Message>Content Redacted – Message content information available
DOH</urn:hl7Message>
            </urn:submitSingleMessage>
        </soap:Body>
</soap:Envelope>
```

Important note to submitting organizations and their vendors regarding section above highlighted in yellow!

Before submitting any immunization reports or immunization queries, submitting organizations and their vendors will receive information for these fields from the DOH WAIIS onboarding team and OneHealthPort. The information is defined below.

- Username – This information is provided by the DOH WAIIS onboarding team.
- Password – This is a password uniquely generated by the DOH WAIIS team and set up at the registry to verify the submitting organization's immunization messages. This information is provided by the DOH WAIIS onboarding team.
- Facility ID – This is an identifier assigned to organizations contracted with the OneHealthPort HIE and is provided to the submitting organization by OneHealthPort.

7.2. Response– xml Sample (Includes header and body)

```
HTTP/1.1 200 OK
Max-Forwards: 20
Via: 1.1 ip-10-10-7-64 ()
Transfer-Encoding: chunked
Connection: keep-alive
X-CorrelationID: Id-c3e29c5cf6e4349973b63a47 0
Accept: application/soap+xml, text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Date: Thu, 28 Mar 2019 15:04:39 GMT
Server: Apache-Coyote/1.1
Content-Language: en-US
Content-Type: application/soap+xml;charset=utf-8

<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope">
    <env:Header/>
    <env:Body>
        <urn:submitSingleMessageResponse xmlns:urn="urn:cdc:iisb:2011">
            <urn:return>Content Redacted – Any message response questions will need to be address
by DOH</urn:return>
        </urn:submitSingleMessageResponse>
    </env:Body>
</env:Envelope>
```

8. ACKNOWLEDGEMENTS AND ERRORS

8.1. AS2 Acknowledgement

Responses to reports or queries received via AS2 connectivity will include:

- Informational content relative to the immunization registry.
- Error content relative to issues identified at the immunization registry.

8.2. Web Services Responses

Web services response codes will return as follows:

- 200 – Success (Message response returns from immunization registry, with an acknowledgment of a reported immunization, a response to a query with immunization information, or error information related to the transactions that successfully reached the registry but encountered an error in processing at the registry such as patient not found, or no registry information available)
- 403 – Certificate Failure (Certificate not recognized error returned by the web services gateway)
- 408 – Timeout Error (Open channel closes before response is received at the web services gateway)
- 503 – (Connectivity Error where web services gateway cannot connect to immunization registry)