

eHealth Ontario

DI Consumer Quick Start Guide

Version 1.2

Revision History

VERSION NO.	DATE	SUMMARY OF CHANGE
V1.0	Dec 5, 2014	First draft
V1.1	Apr 16, 2015	Add ConsentReinstatement service details
V1.2	May 5, 2015	Minor updates based on internal comments

Approval History

APPROVER(S)	TITLE/DEPARTMENT	APPROVED DATE
		YYYY-MM-DD
		YYYY-MM-DD

Table of Contents

1	Introduction	4
1.1	Purpose	4
1.2	Audience	4
1.3	Scope	4
1.4	Assumptions	4
1.5	Feedback	5
2	Contextual Model	6
2.1	Steps	6
2.2	Consumer responsibilities	8
3	Transaction Level Guidelines	10
3.1	SAML token for eHealth access	10
3.2	Registry Stored Query [ITI-18]	11
3.2.1	Find All DI Reports for a Patient	11
3.2.2	Registry Stored Query Response	12
3.3	Retrieve Document Set [ITI-43]	13
3.3.1	Retrieve Single Document	13
3.3.2	Retrieve Document Set Response	14
3.4	Consent Reinstatement	15
3.4.1	Consent Reinstatement Request	15
3.4.2	Consent Reinstatement Response	16
4	Document Content	17
5	OID's	18
6	Unique Provider Identifier's	18
Appendix A.	SAML Information	19
Appendix B.	Transport Specification	19
Appendix C.	DICS iGuide	19
Appendix D.	ConsentServices WSDL	19

eHealth Ontario – DI Consumer Quick Start Guide

1 Introduction

The *eHealth Ontario DI Consumer Quick Start Guide* brings together all the technical requirements and specifications for client software to integrate with eHealth Ontario HIAL services for the purpose of discovering and retrieving diagnostic imaging health records from Ontario's Electronic Health Records (EHR). It describes the pre-requisites and responsibilities of client systems and organizations for successful integration and describes the system to system messages that must be implemented to exchange diagnostic imaging data between the HIAL and client systems.

Implementers wishing to integrate with ehealth Ontario's diagnostic imaging services are required to become familiar with and comply with the general specifications for HIAL integration outlined in *eHealth Ontario HIAL Consumer Implementation Guide – Transport Specification* (See Appendix B). The *DI Consumer Quick Start Guide* (this guide) further refines and qualifies the integration requirements and specifications outlined in the HIAL Consumer Implementation Guide for integration with diagnostic imaging services.

1.1 Purpose

The purpose of this volume is to provide guidelines for the successful integration of consumer applications with eHealth Ontario diagnostic imaging (DI) services.

1.2 Audience

This document is targetted towards implementers – architects, developers, testers – of consumer applications designed to integrate with eHealth Ontario DI services.

1.3 Scope

The scope of this document is to provide a quick startup guide for DI consumer looking to access eHealth's DICS services

The elements covered by this specification volume are:

- Client flow Sequence;
- Creation of ITI-18 and 43 requests;
- Creation of the SAML token

1.4 Assumptions

This implementation guide assumes the reader has some familiarity with the following:

- HL7
- CDA
- XDS

1.5 Feedback

Please send any questions or feedback on this document to architecture@ehealthontario.on.ca.

DRAFT

2 Contextual Model

Figure 1 below depicts a typical pattern of integration between a DI Service Consumer and eHealth Ontario HIAL Services for the purpose of discovering and retrieving diagnostic imaging records from eHealth Ontario's Electronic Health Record (EHR).

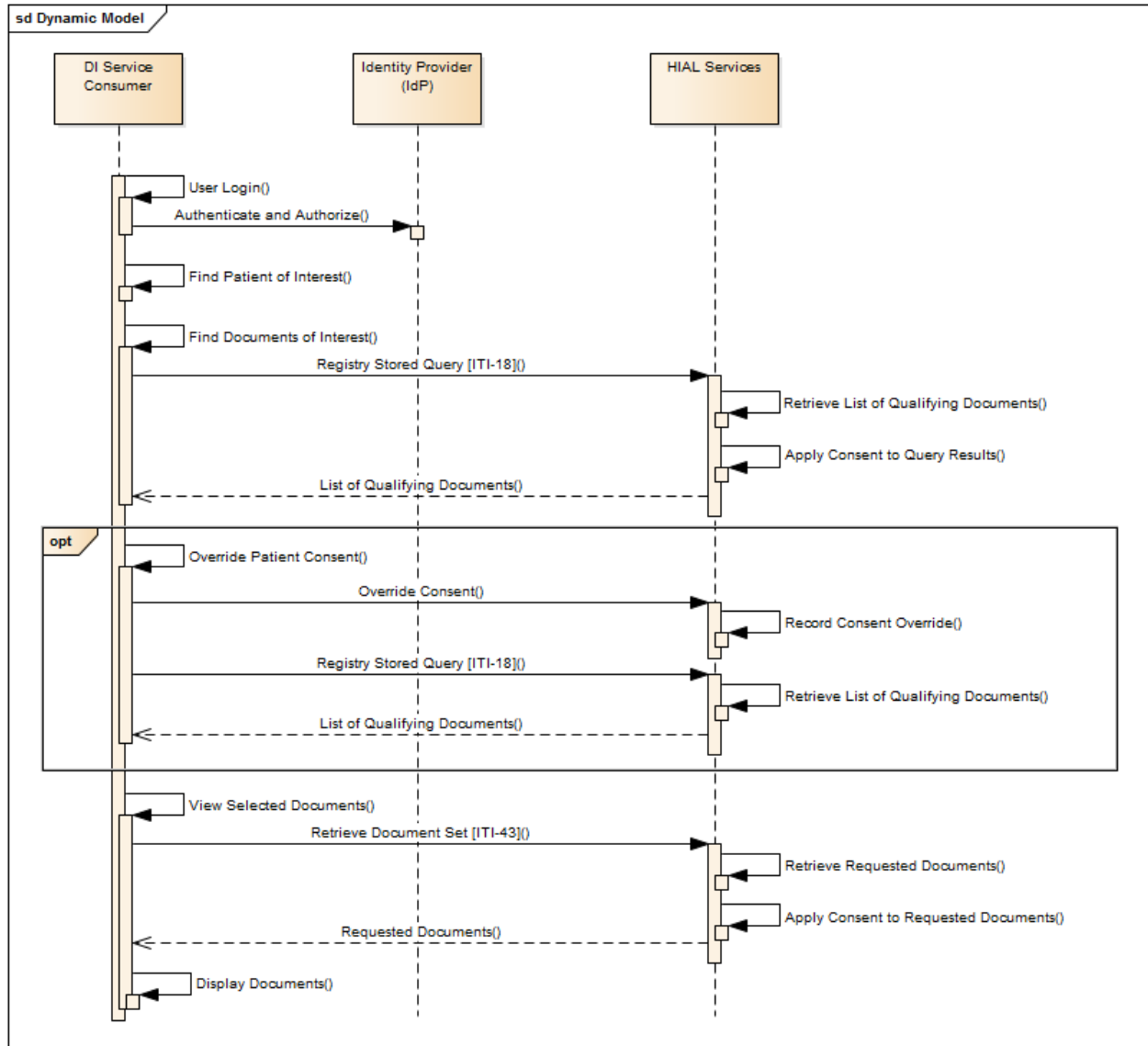


Figure 1: Contextual Interaction Diagram

2.1 Steps

The steps described in the sequence above are as follows:

1. User login + Authenticate and authorize: in these steps, the user is being authenticated and authorized to access DICS reports. For this integration we will assume that the DI Service Consumer is allowed to authenticate and authorize users that will access DICS

reports. eHealth will accept all the credentials authenticated by the DI Service Consumer.

2. DI Service consumer finds the patient. Finding the patient means finding a valid MRN (Medical Record Number) or the HCN (Health Card Number) of the patient of interest (for simplicity, we are assuming in this initial guide that the patient is found by the DI Service Consumer).
3. Create the ITI-18 request: DI Consumer creates the ITI-18 request. The request is a FindDocuments request containing the patient ID (MRN or HCN) for which the documents are required
4. Create the SAML token and add the SAML token to request: DI Consumer creates a SAML token and add that SAML token to the ITI-18 request (see details in the SAML section). The SAML is used by eHO to authenticate and authorize the request. eHO will trust SAML tokens signed by the DI Service Consumer. The SAML will be digitally signed with a OneID issued certificate. This could be the certificate issued for OLIS access. eHealth will have to set the UR trust model for Authentication and Authorization to allow the DI Service Consumer to sign SAML tokens with the certificate issued for OLIS access.
5. DI Consumer send the ITI-18 request: the consumer will have to initiate a Mutual TLS connection with eHealth. For the mutual authentication part, the DI consumer will pass into the TLS connection the TLS certificate issued by OneID for this purpose. For this release, it is possible to use the certificate issued for OLIS access (where available, same as for SAML signature).
6. Display the list of documents and select the document: once the ITI-18 response is received, the DI Consumer will display the list with the documents and will allow the user to select a document of interest.

Note on consent restricted documents: there can be consent directives indicating that none of a patient's documents or some documents are blocked. Those documents will not be returned to the DI Consumer and a Warning will be returned (along with the rest of the documents) indicating this fact. Consumers will have to implement the Consent Override operation if they wish to retrieve documents restricted by consent directives.

7. DI Consumer retrieves the selected document: once the document of interest is selected, the DI Consumer will submit a ITI-43 Retrieve document set transaction. Similarly to the ITI-18 transaction, it will create a SAML token and add it to the request.

8. DI Consumer displays the document: the document is being returned by eHO as a MTOM/XOP optimized attachment. Once the response is received from eHO, the DI consumer will read and display the attachment.

2.2 Consumer responsibilities

The model highlights the following key responsibilities of a DI Service Consumer:

1. All interactions with HIAL Services must be in compliance with the transport specifications outlined in *eHealth Ontario HIAL Consumer Implementation Guide – Transport Specification* (See Appendix B). A key provision of this specification requires service consumers to authenticate and authorize their end users with an identity provider (IdP) that participates in eHealth Ontario's identity management federation. The identity provider can be eHealth Ontario's OneID or any local or regional identity provider that has met the requirements for certification to participate in the eHealth Ontario identity management federation.
2. The DI Service Consumer must include mechanisms for the user or the system to find and select a patient who will be the subject of interest for all interactions with HIAL services. The patient's identity may be conveyed to HIAL Services using a fully qualified MRN, HCN, or an eHealth Ontario enterprise client identifier (ECID). The type of identifier is determined by the assigning authority OID that must be specified along with with id value to form the fully qualified patient identifier.

To convey patient identity using a patient's MRN or HCN, the Assigning Authority must be conveyed as an OID that is issued by eHealth Ontario (see the section on OID's below for details on how to obtain the list of required OID's). To convey patient identity using a patient ECID, the DI Service Consumer will need to obtain this identifier and assigning authority through integration with eHealth Ontario's Provincial Client Registry Service (PCR).

3. The DI Service Consumer must implement the *Registry Stored Query* transaction to query HIAL services for a list of qualifying DI documents that are available in the selected patient's provincial EHR. The query results may be displayed or used by the DI Service Consumer to allow the system or end user to find DI document(s) of interest. If one or more documents were not disclosed by HIAL services due to patient consent, a privacy warning is included in the query results to that effect in which case the DI Service Consumer should provide an appropriate visual cue to inform the end user. Guidelines for implementing this transaction are included in this guide.
4. The DI Service Consumer must implement the *Retrieve Document Set* transaction to retrieve one or more documents of interest from the patient's EHR via HIAL Services. The DI Service Consumer must provide mechanisms for the user or the system to find and select one or more DI documents of interest from the query results retrieved earlier. The identity of the selected document(s) and their location are obtained from the

descriptors (metadata) of the document in the query results and used to retrieve those documents with the Retrieve Document Set transaction. The requested documents are included in the response to the Retrieve Document Set transaction and may be used by the DI Service Consumer or presented to the end user as appropriate. If one or more of the requested documents were not disclosed by HIAL services due to patient consent, a privacy warning is included in the retrieval response to that effect in which case the DI Service Consumer should provide an appropriate visual cue to inform the end user. Guidelines for implementing this transaction are included in this guide.

5. The DI Service Consumer must implement a *Consent Override* transaction if it wishes to support consent override functionality and allow authorized users access to privacy-restricted patient DI records. To support this transaction, the DI Service Consumer must declare who is requesting the override (including substitute decision maker where appropriate), the reason for the override, and the patient (MRN, HCN, or ECID) whose consent is being temporarily re-instated. This may require the DI Service Consumer to prompt the end user to obtain this information prior to issuing the consent override request. Guidelines for implementing this transaction are included in this guide.

Once a consent override has been registered successfully with HIAL Services, it becomes effective for a period of four hours. During this time, a DI Service Consumer may (re)issue a Registry Stored Query or Retrieve Document Set transaction to HIAL Services in order to obtain a complete list of DI documents, including documents that are normally prevented from being disclosed by HIAL Services due to patient consent.

These responsibilities and guidelines for meeting these responsibilities are further described throughout the guide.

3 Transaction Level Guidelines

3.1 SAML token for eHealth access

For Authentication and Authorization to provincial HIAL web services, eHealth Ontario requires a SAML v2.0 security token. The SAML token will have to contain the elements described in the User Registry Attribute Specifications document included in appendix A (*note this SAML specification differs from the provincial SSO SAML specification that may be utilized for federating identity providers*)

For the purpose of integrating early in development with eHealth, we recommend that the DI Consumer use the attached SAML (see appendix A) as a template and replace the following fields (element or attribute):

Element / Attributes	Value	Notes
saml:Issuer	The FQDN of the signing certificate	
dsig:Signature	- Use the signing certificate - Use the digest method specified in the attached SAML (sha1) - Use the exclusive canonicalization algorithm specified in the attached SAML (xml-exc-c14n#) - The signature should be for the SAML assertion element	This element should be generated by the framework used to create the SAML.
saml:Subject/NameID	- Use the FQDN (ID) of the authenticated user	
saml:Subject/NameQualifier	- Use the namespace of the DI Consumer system authentication system	
saml:Conditions	- Make the validity of the SAML 15 minutes	
saml:AuthnStatement/saml:SubjectLocality	- Use DI Consumer system system IP	
saml:AuthnStatement/saml:AuthnContext/saml:AuthnContextDecl/ac:AuthnMethod/ac:Extension/IdentityProvider/AuthenticatingAuthority	- Use the namespace of the DI Consumer system authentication system	
saml:AuthnStatement/saml:AuthnContext/saml:AuthnContextDecl/ac:AuthnMethod/ac:Extension/AssertingParty/AuthenticatingAuthority	- Use the FQDN of the signing certificate (AssertingParty)	
saml:AttributeStatement/saml:Attribute[@name='uid']/saml:AttributeValue	- Use the logged in user ID	
saml:AttributeStatement/saml:Attribute[@name='urn:ehealth:names:if:attribute:AssertingParty']/saml:AttributeValue	- Use the FQDN of the signing certificate (AssertingParty)	
...saml:Attribute[@name='urn:ehealth:names:if:attribute:lastName']/saml:AttributeValue	- Last Name of the User (if available, if not, leave it empty)	
...saml:Attribute[@name='urn:ehealth:names:if:attribute:obo']/saml:AttributeValue	- Leave empty (On Behalf Of)	
...saml:Attribute[@name='urn:ehealth:names:if:attribute:uao']/saml:AttributeValue	- Must be present, use the UPI of the Hospitalsending the request. Use the format from the sample: "urn:ehealth:rid:upi:102544111416"	
...saml:Attribute[@name='urn:ehealth:names:if:attribute:realIdentity']/saml:AttributeValue	- Real identity of the user	

:attribute:rid]/saml:AttributeValue		
	-	

Please see appendix A for the detailed SAML specification along with a sample SAML token. Also please refer to the section on UPI's for details on how to obtain the necessary provider UPI's from eHealth Ontario.

3.2 Registry Stored Query [ITI-18]

The Registry Stored Query transaction supports a variety of queries to find and retrieve the metadata associated with published documents in the XDS Document Registry. While the transaction also supports finding metadata information for submission sets, folders, and associations, this section will focus on the most common expected use case for consumers of the system (i.e. finding document's of interest).

This section shows examples of the of the Registry Stored Query transaction to issue FindDocuments queries to locate diagnostic imaging reports of interest.

Implementers can review the attached iGuide (see Appendix C) to see a complete list of all possible query types and query parameters for this transaction.

3.2.1 Find All DI Reports for a Patient

The following sample transaction will query the XDS registry for all active (non-deprecated) diagnostic imaging reports for the patient having an MRN of '1234' from a hospital with a defined assigning authority OID of '1.2.3.4.5' (see Appendix XX for listing of MRN assigning authorities)

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope
  xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
  xmlns:wsa="http://www.w3.org/2005/08/addressing">
  < soap:Header>
    <Security xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <!-- Insert SAML Token here (see section 3.1)-->
      ...
    </Security>
    <wsa:Action s:mustUnderstand="1">urn:ihe:iti:2007:RegistryStoredQuery</wsa:Action>
    <!-- The following should be a unique value for each transaction -->
    <wsa:MessageID>urn:uuid:a02ca8cd-86fa-4afc-a27c-616c183b2055</wsa:MessageID>
    <wsa:ReplyTo>
      <wsa:Address>http://www.w3.org/2005/08/addressing/anonymous</wsa:Address>
    </wsa:ReplyTo>
    <wsa:To s:mustUnderstand="1">https://gateway.ehealthontario.on.ca:7180/index/services/registry</wsa:To>
  </soap:Header>
  <soap:Body>
    <query:AdhocQueryRequest
      xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
      xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0"
      xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0">
      <query:ResponseOption returnComposedObjects="true" returnType="LeafClass"/>
      <!-- The following is the fixed value to specify the FindDocuments query -->
      <rim:AdhocQuery id="urn:uuid:14d4debf-8f97-4251-9a74-a90016b0af0d">
        <!-- Patient ID is mandatory -->
        <rim:Slot name="$XDSDocumentEntryPatientId">
```

```

        <rim:ValueList>
          <rim:Value>'1234^^^&1.2.3.4.5&ISO'</rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <!-- Status query parameter (mandatory) -->
      <rim:Slot name="$XDSDocumentEntryStatus">
        <rim:ValueList>
          <rim:Value>('urn:oasis:names:tc:ebxml-regrep:StatusType:Approved')</rim:Value>
        </rim:ValueList>
      </rim:Slot>
      <!-- ClassCode query parameter (optional) -->
      <rim:Slot name="$XDSDocumentEntryClassCode">
        <rim:ValueList>
          <!-- The following value is for Diagnostic Imaging Reports -->
          <rim:Value>('18748-4^^2.16.840.1.113883.6.1')</rim:Value>
        </rim:ValueList>
      </rim:Slot>
    </rim:AdhocQuery>
  </query:AdhocQueryRequest>
</s:Body>
</s:Envelope>

```

3.2.1.1 Narrow Search by Time

In addition to restricting the documents to only DI reports, one of the other most common optional search parameters used is to specify the earliest time for which documents should be included. For example it is possible to only query documents in the last day, month, year, etc. The specified value can include a time component if required which must be specified in UTC format. Note it is also possible to specify the end date/time if so desired as well.

For example, the following slot can be added to the sample query above to further restrict the returned documents to only include those created since December 1, 2014.

```

      <!-- CreationStartTime parameter (optional) -->
      <rim:Slot name="$XDSDocumentEntryCreationTimeFrom">
        <rim:ValueList>
          <!-- The following value is for Diagnostic Imaging Reports -->
          <rim:Value>'20141201'</rim:Value>
        </rim:ValueList>
      </rim:Slot>

```

3.2.2 Registry Stored Query Response

A sample Registry Stored Query response message is shown below. This sample response contains 2 ExtrinsicObjects where each one maps to a given document in the XDS repository. In general, a response may contain 0 or more ExtrinsicObjects based on your search criteria. For simplicity, the detailed contents of these ExtrinsicObjects are omitted other than the information necessary in the first one to retrieve the document associated from the XDS repository. Please refer to the iGuide specification to see a complete example as well as details about each of the attributes included.

```

<s:Envelope
  xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>

```

```

<a:Action>urn:ihe:iti:2007:RegistryStoredQueryResponse</a:Action>
<a:RelatesTo>urn:uuid:a02ca8cd-86fa-4afc-a27c-616c183b2055</a:RelatesTo>
</s:Header>
<s:Body>
  <query:AdhocQueryResponse
    xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
    <rim:RegistryObjectList xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
      <rim:ExtrinsicObject ... >
        <!-- Contents of ExtrinsicObject mostly omitted -->
        ...
        <rim:Slot name="repositoryUniqueId">
          <rim:ValueList>
            <rim:Value>2.16.840.1.113883.3.239.30.1</rim:Value>
          </rim:ValueList>
        </rim:Slot>
        ...
        <rim:ExternalIdentifier
          id="urn:uuid:c3fcfb0e-9765-4f5b-abaa-b37ac8ff05a5"
          registryObject="urn:uuid:08a15a6f-5b4a-42de-8f95-89474f83abdf"
          identificationScheme="urn:uuid:2e82c1f6-a085-4c72-9da3-8640a32e42ab"
          value="2.16.840.1.113883.3.239.23.7.2043249">
            <rim:Name>
              <rim:LocalizedString value="XSDDocumentEntry.uniqueId"/>
            </rim:Name>
          </rim:ExternalIdentifier>
        </rim:ExtrinsicObject>
        <rim:ExtrinsicObject ... >
          <!-- Contents of second ExtrinsicObject entirely omitted -->
        </rim:ExtrinsicObject>
      </rim:RegistryObjectList>
    </query:AdhocQueryResponse>
  </soapenv:Body>
</soapenv:Envelope>

```

Note: the highlighted values for the repository unique Id and document Id will be used in the ITI-43 request to retrieve the corresponding document.

3.3 Retrieve Document Set [ITI-43]

The Retrieve Document Set transaction is used to retrieve one or more documents from the XDS repository. The documents are identified by their 'uniqueId' attribute along with the id of the repository in which they are contained (both of these values can be obtained from the results of the ITI-18 transaction, see the ITI-18 response, highlighted values).

Note that unlike the Registry Stored Query request and reply messages, the Retrieve Document Set transaction requires the use of multipart MTOM/XOP HTTP messages. Please see the transport specification in Appendix B for more details.

3.3.1 Retrieve Single Document

```

<s:Envelope
  xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <Security xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <!-- Insert SAML Token here (see section 3.1)-->
    </Security>
    <a:Action s:mustUnderstand="1">urn:ihe:iti:2007:RetrieveDocumentSet</a:Action>
    <a:MessageID>urn:uuid:0fbfdced-6c01-4d09-a110-2201afedaa02</a:MessageID>
    <a:ReplyTo>
      <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
    </a:ReplyTo>
    <a:To s:mustUnderstand="1">https://gateway.ehealthontario.on.ca:7180/index/services/repository </a:To>
  </s:Header>
  <s:Body>
    <RetrieveDocumentSetRequest xmlns="urn:ihe:iti:xds-b:2007">
      <DocumentRequest>
        <RepositoryUniqueid>2.16.840.1.113883.3.239.30.1</RepositoryUniqueid>
        <DocumentUniqueid>2.16.840.1.113883.3.239.18.151.2043249</DocumentUniqueid>
      </DocumentRequest>
    </RetrieveDocumentSetRequest>
  </s:Body>
</s:Envelope>

```

3.3.2 Retrieve Document Set Response

```

<s:Envelope
  xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://www.w3.org/2005/08/addressing">
  <s:Header>
    <a:Action s:mustUnderstand="1">urn:ihe:iti:2007:RetrieveDocumentSetResponse</a:Action>
    <a:RelatesTo>urn:uuid:0fbfdced-6c01-4d09-a110-2201afedaa02</a:RelatesTo>
  </s:Header>
  <s:Body>
    <RetrieveDocumentSetResponse
      xmlns="urn:ihe:iti:xds-b:2007"
      xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0">
      <rs:RegistryResponse
        status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success"
        xmlns:rs="urn:oasis:names:tc:ebxml-regrep:xsd:rs:3.0">
      </rs:RegistryResponse>
      <DocumentResponse>
        <RepositoryUniqueid>2.16.840.1.113883.3.239.30.1</RepositoryUniqueid>
        <DocumentUniqueid>2.16.840.1.113883.3.239.18.151.2043249</DocumentUniqueid>
        <mimeType>text/xml</mimeType>
        <Document>
          <!-- reference to MTOM/XOP attachment containing CDA document -->
          <xop:Include
            href="cid:1.urn:uuid:AFBE87CB65FD88AC4B1220879854123@apache.org"
            xmlns:xop="http://www.w3.org/2004/08/xop/include"/>
          </xop:Include>
        </Document>
      </DocumentResponse>
    </RetrieveDocumentSetResponse>
  </s:Body>
</s:Envelope>

```

```
</s:Body>
</s:Envelope>
```

3.4 Consent Reinstatement

In situations where the patient has put a consent directive in place, any consumer queries for that patient's data may result in one or more records (depending on the consent directive) being withheld. In the event that any data is withheld during an ITI-18 request, a warning will be included as part of the ITI-18 response to inform the requesting application that not all results have been returned. The following XML fragment shows an ITI-18 response where consent has been applied:

```
<query:AdhocQueryResponse xmlns:query="urn:oasis:names:tc:ebxml-regrep:xsd:query:3.0"
    status="urn:oasis:names:tc:ebxml-regrep:ResponseStatusType:Success">
  <RegistryErrorList highestSeverity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning">
    <RegistryError errorCode="XDSConsentApplied"
      codeContext="Documents were not returned due to an applied consent directive"
      severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning"/>
    <!-- Depending on the type of consent directive, the following warning may also be returned -->
    <RegistryError errorCode="XDSPatientConsentDirective"
      codeContext="There is a consent directive in place for the selected patient"
      severity="urn:oasis:names:tc:ebxml-regrep:ErrorSeverityType:Warning"/>
  </RegistryErrorList>
  <rim:RegistryObjectList xmlns:rim="urn:oasis:names:tc:ebxml-regrep:xsd:rim:3.0">
    <!-- Depending on the type of consent directive, 0 or more documents may be returned -->
  </rim:RegistryObjectList>
</query:AdhocQueryResponse>
```

In these situations, the consumer application should ensure that it presents a warning to the user to notify them that they are not viewing all the records available for the specified patient. The application may allow the user to request the consent be overridden in cases where the patient (or the appropriate substitution decision maker) has given the user permission to do so. The custom Consent Reinstatement web service provides this capability and allows the user access to the results for the next 4 hours. Any subsequent ITI-18 or ITI-43 requests where the user id and provider organization UPI contained in the SAML token match those contained in the Consent Reinstatement request will be allowed access to the data. Sample request and response messages are shown below and the complete WSDL and XSD files can be found in the appendix.

3.4.1 Consent Reinstatement Request

```
<s:Envelope xmlns:s="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:a="http://www.w3.org/2005/08/addressing"
  xmlns:v01="http://ehealthontario.on.ca/xmlns/consent/v01">
  <s:Header>
    <Security xmlns="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
      <!-- Insert SAML Token here (see section 3.1)-->
    </Security>
    <a:Action s:mustUnderstand="1">
      http://ehealthontario.on.ca/xmlns/consent/v01/ConsentReinstatementRequest
    </a:Action>
    <a:MessageID> urn:uuid:58F88C76251428C13D1377795950673 </a:MessageID>
```

```

<a:ReplyTo>
  <a:Address>http://www.w3.org/2005/08/addressing/anonymous</a:Address>
</a:ReplyTo>
<a:To s:mustUnderstand="1">
  https://gateway.ehealthontario.on.ca:7180/ConsentRegistryService/V01
</a:To>
</s:Header>
<s:Body>
  <v01:ConsentReinstatementRequest>
    <v01:User>
      <v01:FirstName>User_FirstName</v01:FirstName>
      <v01:LastName>User_LastName</v01:LastName>
      <!--The specified Provider Id must match one of the eHealth Ontario
      provider UPI's that will be provided -->
      <v01:ProviderId root="2.16.840.1.113883.3.239.9" extension="444"/>
    </v01:User>
    <v01:Patient>
      <!--The specified Patient Id can be an MRN, HCN, or EID similar to the
      other DICS web services detailed in the iGuide -->
      <v01:PatientId root="2.16.840.1.113883.3.239.20" extension="1606"/>
      <!--Optional:-->
      <v01:SubstituteDecisionMaker>
        <v01:FamilyName>SDM_FamilyName</v01:FamilyName>
        <!--Optional:-->
        <v01:GivenName>SDM_GivenName</v01:GivenName>
        <!--Optional:-->
        <v01:RelationshipToPatient>SDM_RelationshipToPatient</v01:RelationshipToPatient>
      </v01:SubstituteDecisionMaker>
    </v01:Patient>
  </v01:ConsentReinstatementRequest>
</s:Body>
</s:Envelope>

```

Note that the provider id specified in the above sample (444), must match one of the eHealth Ontario provider UPI's. Please refer to the section on UPI's for more details on how to obtain these UPI's.

3.4.2 Consent Reinstatement Response

```

<s:Envelope
  xmlns:s="http://www.w3.org/2003/05/soap-envelope"
  xmlns:a="http://www.w3.org/2005/08/addressing"
  xmlns:v01="http://ehealthontario.on.ca/xmlns/consent/v01">
  <s:Header>
    <a:Action s:mustUnderstand="1">
      http://ehealthontario.on.ca/xmlns/consent/v01/ConsentReinstatementResponse
    </a:Action>
    <a:RelatesTo> urn:uuid:58F88C76251428C13D1377795950673</a:RelatesTo>
  </s:Header>
  <s:Body>
    <v01:ConsentReinstatementResponse>
      <v01:Acknowledgement>SUCCESS</v01:Acknowledgement>
    </v01:ConsentReinstatementResponse>
  </s:Body>
</s:Envelope>

```


Ankle Right 4V or more
C000008736QOQ

This patient fell and hurt his left foot.
We took a lot of images.

That is all.

Reported By: House, Gregory MD
Signed By: House, Gregory MD 25/10/13

cc:
Foreman, Eric
Wilson, James MD

D: 25/10/13 1041
T: 25/10/13 1042 (QCDORE)

5 OID's

When specifying the patient identifier for the RegistryStoredQuery [ITI-18] service, a fully qualified id must be provided. This includes the alpha-numeric id value along with an OID qualifier that represents the assigning authority responsible for issuing this id.

When health card numbers are to be used for the patient identifier (note that only Ontario health card numbers are supported), the following OID should be used as the assigning authority:

2.16.840.1.113883.4.59

When enterprise id's are to be used for the patient identifier (requires integration with pCR), the following OID should be used as the assigning authority:

2.16.840.1.113883.3.239.20

When MRN's are to be used for the patient identifier, the OID associated with the hospital from which the MRN was generated should be used as the assigning authority. To obtain this list of OID's, please send an email to architecture@ehealthontario.on.ca and specify the list of hospitals for which you need the corresponding assigning authority OID's.

6 Unique Provider Identifier's

When specifying the identifier for the hospital organization for which a provider is working under the authority of (UAO), the Unique Provider Identifier (UPI) number as defined by eHealth Ontario must be provided. To obtain the list of UPI's for all the organizations for which you will have providers access the system, please send an email to architecture@ehealthontario.on.ca requesting these UPI's.

Appendix A. SAML Information

The SAML specification, required to be utilized for all web service interactions with the provincial HIAL, is attached below along with a sample SAML token based on this specification.



User Registry
Attribute Specification



saml2.xml

Appendix B. Transport Specification

The transport specification, required to be utilized for accessing the DICS web services, is attached below.



eHealth Ontario -
CIG-HIAL Transport s

Appendix C. DICS iGuide

For details on the CDA document format and the XDS services utilized, please reference the iGuide specification that can be downloaded as part of the DICS package from the following link.

<http://www.ehealthontario.on.ca/en/standards/view/diagnostic-imaging-common-service-standard-dinbspcs/>

Please note that the XDS services utilized are based on the standard XDS WSDL and schema files that can be downloaded from the following IHE ftp site:

ftp://ftp.ihe.net/TF_Implementation_Material/ITI/

Appendix D. ConsentServices WSDL

The attached WSDL and XSD files provide the details required for the ConsentReinstatement web service.



ConsentService.wsdl



eho-consent.xsd