EMR EHR Connectivity 2.1

Transport Layer Interoperability – Requirements

July 13, 2020
Document Version & Status: 1.1 – DFC (Draft for Comment)

Table of Contents

1. INTRODUCTION 3

1.1 OVERVIEW 3
1.2 VERSION HISTORY 3
1.3 SCOPE 3
1.3.1 In Scope 3
1.4 RELATED DOCUMENTS, REFERENCES AND SOURCES 3

2. EMR REQUIREMENTS 4

2.1 PUBLIC KEY INFRASTRUCTURE CERTIFICATE 4
2.2 HTTP/HTTPS HEADERS 6
2.3 MESSAGE DELIVERY 7
2.3.1 Example GET Request 8
2.3.2 Example POST Request 8
2.4 ERROR HANDLING 9
2.4.1 HTTPS Errors 11
2.4.2 SOAP Errors 11
2.4.3 Resubmission of Failed Transactions (Queuing and Retry) 17
2.4.4 EMR Offering Reliability 17
2.5 LOGGING AND AUDITING 18

3. APPENDIX A: GLOSSARY OF KEY TERMS AND DEFINITIONS 20

3.1 ACRONYMS AND ABBREVIATIONS 20
3.2 DEFINITIONS 20

1. INTRODUCTION

1.1 Overview

The purpose of this document is to provide EMR vendors with implementation guidance and functional requirements to implement the Transport Layer Interoperability (TLI) portion of Ontario Health Digital Services (OHDS) HIAL Transport and Message Specification. The goal is to provide details for an EMR Offering to be able to establish a connection with the provincial Health Information Access Layer (HIAL).

1.2 Version History

VERSION	REVISION DATE	REVISION NOTES
1.0	2019-12-23	a) Updated TLI02.01 to deprecate support for TLS v1.1 b) Updated TLI02.04 to clarify that the CRL needs to be only checked, and not necessarily maintained
1.1	2020-07-13	a) Added TLI04.08 for user registry tokens. The requirement was previously in Federated ID & SSO b) Re-added TLI05.01 that was missing.

~~1.1~~1.3 Scope

~~1.1.1~~1.3.1 In Scope

- Requirements for EMR Offerings to implement TLI to interact with the provincial HIAL to support EHR services that reside on it.

~~1.3~~1.4 Related Documents, References and Sources

ID	NAME	VERSION	DATE PUBLICATION
1	HIAL Transport and Message Specification Integration Guide (Ontario Health Digital Services, 2018) https://www.ehealthontario.on.ca/en/standards/view/hial-transport-message-specification	1.4	2018-07-12

2. EMR REQUIREMENTS

This section consists of the EMR functional requirements for TLI.
Support:
M = Mandatory. EMR Offerings certified for this specification MUST support this requirement
O = Optional. EMR vendors MAY choose to support this requirement in their certified EMR Offering

Status:
N = New requirement for this EMR Specification
P = Previous requirement
U = Updated requirement from the previous EMR Specification version
R = Retired requirement from previous EMR Specification version

OMD #:
A unique identifier that identifies each requirement within OntarioMD's EMR Requirements Repository

CONFORMANCE LANGUAGE
The following definitions of the conformance verbs are used in this document:

- **SHALL/MUST** – Required/Mandatory
- **SHOULD** – Best Practice/Recommendation
- **MAY** – Acceptable/Permitted

The tables that follow contain column headings named: 1) "Requirement," which generally contains a high-level requirement statement; and 2) "Guidelines," which contains additional instructions or detail about the high-level requirement. The text in both columns is considered requirement statements.

2.1 Public Key Infrastructure Certificate

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
TLI01.01	The EMR Offering MUST use an assigned public key infrastructure (PKI) certificate	During the registration process for each EMR deployed to a practice, OHDS issues a unique system-level PKI certificate that MUST be installed on each EMR and used to connect to the provincial HIAL.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	to establish a connection to the provincial HIAL.			
TLI01.02	The EMR Offering MUST support PKI certificates based on Secure Hash Algorithm 2 (SHA2) security algorithms.		M	P
TLI01.03	The EMR Offering MUST trust the OHDS Certificate Authority (CA).	**Note**: The trusted CA certificate is owned and managed by OHDS.	M	P

2.2 HTTP/HTTPS Headers

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
TLI02.01	The EMR Offering MUST establish the connection to the provincial HIAL via a mutually authenticated HTTPS connection using the TLS/SSL protocol.	Mutual authentication MUST support: a) TLS v1.2 b) 2048-bit certificates and the SHA2 signing algorithm **Note**: TLS v1.1 is no longer supported.	M	U
TLI02.02	The EMR Offering MUST implement supported HTTP compression methods.	The provincial HIAL supports HTTP message compression. This is helpful when exchanging messages to reduce network bandwidth. The EMR Offering MUST support both HTTP compression methods: a) gzip b) deflate HTTP message compression is indicated through the following HTTP headers: a) **Accept-Encoding** indicates what HTTP compression method the EMR Offering supports b) **Content-Encoding** indicates what HTTP compression method the EMR Offering uses to send the request	M	P
TLI02.03	The EMR Offering MUST provide a custom HTTP header with the client transaction ID call *ClientTxID* in HTTP headers.	The client transaction ID MUST be unique and will be used during troubleshooting and auditing to identify the transaction from the point of view of the EMR Offering.	M	P
TLI02.04	The EMR Offering MUST perform server certificate revocation checks against the Certificate Revocation List (CRL).	The EMR Offering MUST be able to check an up-to-date CRL within the validity period defined by the CRL. **Note**: The CRL is published by OHDS.	M	U

2.3 Message Delivery

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
TLI03.01	The EMR Offering MUST comply with all requirements identified in the *HIAL Transport and Message Specification Integration Guide.*	Refer to the HIAL Transport and Message Specification Integration Guide.	M	P
TLI03.02	The EMR Offering MUST communicate with the provincial HIAL using immediate (synchronous request-response) response message pattern.	Queued (polling) mode and deferred (asynchronous) message patterns are not supported.	M	P

The following are examples of a GET and a POST request with HTTP headers.

2.3.1 Example GET Request

```
GET https://wsgateway.prod.ehealthontario.ca:port/API/FHIR/ExampleService/v1/… HTTP/1.1

Accept-Encoding: gzip,deflate
Accept: application/json+fhir
ClientTxtID: 12345
Authorization: BearerPHNhbWw6QXNzZXJ0aW9uIElEPSJJRGU5Nzc0ODMzLTI0ODQtNGE4Ni04OWQwLWZmNz…
Host: 10.69.0.110:38080
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
```

2.3.2 Example POST Request

```
POST https://wsgateway.prod.ehealthontario.ca:port/API/FHIR/ ExampleService /v1/… HTTP/1.1

Accept-Encoding: gzip,deflate
Content-Type: application/json+fhir
ClientTxtID: 12345
Authorization: BearerPHNhbWw6QXNzZXJ0aW9uIElEPSJJRGU5Nzc0ODMzLTI0ODQtNGE4Ni04OWQwLWZmNz…
Content-Length: 1654
Host: host:10.69.0.110:38080
Connection: Keep-Alive
User-Agent: Apache-HttpClient/4.1.1 (java 1.5)
```

2.4 Error Handling

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
TLI04.01	The EMR Offering MUST take appropriate actions for all errors (as defined throughout the subsections of 1.5 - Error Handling) that can occur while communicating with the provincial HIAL.	At a minimum, the categories of errors the EMR Offering MUST identify include: a) **Transmission errors**: Errors that occur when the EMR Offering cannot access or connect to the provincial HIAL. b) **Security and non-conformance related errors**: Errors that occur when incorrect security elements or non-conformant request messages are used for communication with the provincial HIAL. c) **Unspecified errors**: Errors that occur when the provincial HIAL experiences internal problems.	M	P
TLI04.02	The EMR Offering MUST implement a fallback strategy if one or more errors prevent the submission of a transaction to the provincial HIAL.	The fallback strategy may include resubmitting the unsuccessful transaction until the error condition is resolved.	M	P

To consume EHR services, EMR Offerings will also have to support application errors that are specific to the EHR service. Application errors are typically related to HL7 v2, v3 and FHIR responses to interactions or other proprietary application errors for non-HL7 interactions. These application errors are specific to each EHR service and are defined in their respective implementation guides.

From a transport layer perspective, the categories of errors will manifest themselves as one of the following transport layer constructs:

CATEGORY OF ERROR	TRANSPORT LAYER CONSTRUCT
Transmission	• HTTPS
Security and non-conformance	• HTTPS – mutual authentication • Simple Object Access Protocol (SOAP) – User authentication and authorization
Unspecified errors	• SOAP

Note: Each category may have its own set of specific errors.

2.4.1 HTTPS Errors

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
TLI04.03	The EMR Offering MUST follow HTTP and TLS/SSL general guidelines when handling HTTPS exceptions.	HTTPS errors can occur in the following circumstances: a) When the provincial HIAL is not accessible b) When there is a problem with the EMR Offering's TLS/SSL client certificate. TLS/SSL client certificate issues can range from using an invalid, expired or revoked certificate, or not using a certificate when attempting to connect to the provincial HIAL. Regardless of the type of error, the EMR Offering MUST be configurable to set the number of connection retries and time interval between unsuccessful connection attempts. Upon each unsuccessful attempt, the EMR Offering MUST interpret the corresponding HTTPS exception based on HTTP guidelines. If there is an HTTPS handshake exception, the cause may be that the TLS/SSL client certificate is missing, expired, revoked or it is invalid. The organization that provides support for the EMR Offering (e.g., EMR vendor or third-party service provider) should check that the TLS/SSL client certificate is valid. If the TLS/SSL client certificate appears valid but is not functioning properly, or if the certificate needs to be replaced, the EMR Offering support organization will need to contact the OHDS service desk to determine if the appropriate client certificate is being used.	M	P

2.4.2 SOAP Errors

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
TLI04.04	The EMR Offering MUST NOT send non-conformant web service requests once they have passed the conformance tests.	A non-conformant message is treated as a threat by the provincial HIAL and will be rejected accordingly.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
TLI04.05	The EMR Offering MUST respond appropriately to the SOAP 1.1 fault codes and fault strings, and SOAP 1.2 code and reason.	See the Handling Soap Errors section of this document for handling SOAP errors for more detailed information and the corresponding EMR system actions.	M	P

2.4.2.1 Handling SOAP errors

SOAP errors can occur in the following circumstances:

- Authentication and authorization errors
- Requests are not conformant with the web services policy such as:
    - Schema validation errors
    - Missing required header elements
    - Non-conformant web service requests
- Internal errors resulting from system error conditions (such as backend connectivity issues)

SOAP errors are returned to the EMR Offering in the form of a <faultcode> and <faultstring> combination within the SOAP <fault> element. EMR Offerings MUST be able to correctly handle all SOAP errors. The SOAP 1.1 fault element has the following sub-elements.

SUB-ELEMENT	DESCRIPTION
<faultcode>	A code for identifying the fault
<faultstring>	A human-readable explanation of the fault
<faultactor>	Not used by the provincial HIAL
<detail>	Not used by the provincial HIAL

SOAP 1.1 Fault Codes:

ERROR	DESCRIPTION
Client	The message was incorrectly formed or contains incorrect information
Server	There was a problem with the server so the message could not proceed
VersionMismatch	Not used by the provincial HIAL
MustUnderstand	Not used by the provincial HIAL

The SOAP 1.2 Fault element has the following sub-elements:

SUB-ELEMENT	DESCRIPTION
<Code>/<Value>	A code for identifying the fault (Sender or Receiver)
<Reason>/<Text>	A human-readable explanation of the fault

SOAP 1.2 Fault Codes:

ERROR	DESCRIPTION
Sender	The message was incorrectly formed or contains incorrect information
Receiver	There was a problem with the server so the message could not proceed

The following are examples of SOAP errors returned by the provincial HIAL:

RETURNED SOAP 1.1 ERROR	RETURNED SOAP 1.2 ERROR	POSSIBLE CAUSE	EMR OFFERING ACTION
Faultcode: Client Faultstring: Rejected by policy Sample: <env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"> <env:Body> <env:Fault> <faultcode>env:Client</faultcode> <faultstring>Rejected by policy (from client)</faultstring> </env:Fault> </env:Body> </env:Envelope>	Code: Sender Reason: Rejected by policy Sample: <env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope"> <env:Body> <env:Fault> <env:Code> <env:Value>env:Sender</env:Value> </env:Code> <env:Reason> <env:Text xml:lang="en-US">Rejected by policy (from client)</env:Text> </env:Reason> </env:Fault> </env:Body> </env:Envelope>	Authorization and authentication failures: 1. Client certificate does not have appropriate grants 2. Missing Security Assertion Markup Language (SAML) token 3. Expired SAML token 4. SAML token certificate is revoked 5. Asserted user identity doesn't have the appropriate grants	Retry: no
Faultcode: Client Faultstring: Internal server error Sample:	Code: Sender Reason: Internal server error Sample:	1. Schema validation 2. Missing conformance elements such as WS-Addressing elements as per this specification 3. Incorrect routing information	Retry: no

RETURNED SOAP 1.1 ERROR	RETURNED SOAP 1.2 ERROR	POSSIBLE CAUSE	EMR OFFERING ACTION
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"> <env:Body> <env:Fault> <faultcode>env:Client</faultcode> <faultstring>Internal Server Error</faultstring> </env:Fault> </env:Body> </env:Envelope>	<env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope"> <env:Body> <env:Fault> <env:Code> <env:Value>env:Sender</env:Value> </env:Code> <env:Reason> <env:Text xml:lang="en-US"> Internal Error (from client)</env:Text> </env:Reason> </env:Fault> </env:Body> </env:Envelope>		
Faultcode: Server Faultstring: Internal server error Sample: <env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/"> <env:Body> <env:Fault> <faultcode>env:Server</faultcode> <faultstring>Internal Server Error</faultstring>	Code: Receiver Reason: Internal server error Sample: <env:Envelope xmlns:env="http://www.w3.org/2003/05/soap-envelope"> <env:Body> <env:Fault> <env:Code> <env:Value>env:Receiver</env:Value> </env:Code>	1. Internal connectivity issues (for example from HIAL to Service) 2. Internal issues (failure of internal HIAL components)	Retry: yes, three times with a three-second delay between trials

RETURNED SOAP 1.1 ERROR	RETURNED SOAP 1.2 ERROR	POSSIBLE CAUSE	EMR OFFERING ACTION
</env:Fault> </env:Body> </env:Envelope>	<env:Reason> <env:Text xml:lang="en-US">Internal Error (from server)</env:Text> </env:Reason> </env:Fault> </env:Body> </env:Envelope>		

2.4.3 Resubmission of Failed Transactions (Queuing and Retry)

EMR Offerings may encounter issues when sending requests to the provincial HIAL. Some requests may not be submitted in real-time or out of order. The provincial HIAL does not offer a facility for resubmission of failed transactions or any logical or chronological ordering of transactions.

2.4.4 EMR Offering Reliability

EMR Offerings communicate with the provincial HIAL using a request-reply message pattern. Upon receiving a request from the EMR Offering, the provincial HIAL will synchronously reply with the corresponding response.
If the response is not received, or a transport exception has occurred, the EMR Offering will have to resubmit the same request using the same client transaction ID.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
TLI04.06	The EMR Offering MUST use the same message ID as in the original request message only when resending messages.	EMR Offerings MUST NOT reuse message IDs unless they are resubmitting a failed request. If a duplicate transaction is sent to the provincial HIAL, the original response may be returned when available.	M	P

2.4.4.1 Duplicate Messages – message ID

Each request message sent by the EMR Offering has a unique client transaction ID, which identifies the message. This message ID, along with the Sending Application Identifier may be used by the provincial HIAL to identify duplicate messages and avoid processing them again.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
TLI04.07	The EMR Offering MUST ensure that the message ID is unique.	EMR Offerings MUST NOT reuse message IDs unless they are resubmitting a failed request.	M	P

2.4.4.2 Non-repudiation

Non-repudiation is achieved through:

- Mutual authentication between the EMR Offering and provincial HIAL using both the client and server TLS/SSL certificates to identify the sending and receiving systems.
- The client-signed SAML security token that is asserted by the User Registry. This process identifies the clinical authority that created the transaction. Refer to the "Federation Identity and Single Sign-On" artifact within this EMR specification for more information about the use of SAML security tokens.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
TLI04.08	The EMR Offering MUST use the UR Client Token (Token 2) to assert an EMR user's identity when accessing provincial EHR solutions and EHR services.	The EMR Offering MUST present the User Registry Client Token (Token 2) each time an EHR service is launched. The EMR Offering MUST use the same UR Client Token (Token 2) when accessing different EHR services within the validity period of the Federation SSO session.	M	N

2.5 Logging and Auditing

EMR systems log different information and interactions. In some instances, PHI may be passed as parameters of the interaction. As a result, precaution should be taken to log only what is necessary, to avoid unintentionally saving and/or providing access to PHI.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
TLI05.01	The EMR Offering MUST log timestamps for successful and failed transactions with the provincial HIAL.	At a minimum, the following information MUST be logged: a) Date and time transaction initiated b) The user or system attempting the transaction c) Transaction attempted by the user or system d) Status of the message (e.g., success or failure) e) provincial HIAL Message identifier(s) Additional information SHOULD be logged within the EMR, as necessary, to facilitate troubleshooting and auditing.	M	P
TLI05.02	The EMR Offering MUST log timestamps for successful and failed transactions with any EHR service.	At a minimum, the following information MUST be logged: f) Date and time transaction initiated g) The user or system attempting the transaction h) Transaction attempted by the user or system i) Status of the message (e.g., success or failure) j) provincial HIAL Message identifier(s) k) Name of EHR service Additional information SHOULD be logged within the EMR, as necessary, to facilitate troubleshooting and auditing.	M	P
TLI05.03	The EMR Offering MUST log timestamps for transactions for each EHR service, in accordance with agreements with the Service Provider.	EMR Offering requirements for logging and auditing may be described through federation agreements between the organization responsible for the EHR service and each consumer application system.	M	P

3. APPENDIX A: GLOSSARY OF KEY TERMS AND DEFINITIONS

3.1 Acronyms and Abbreviations

This table identifies definitions for terms used within or that are relevant to this document.

ACRONYM	DEFINITION
CRL	Certificate Revocation List
EHR	Electronic Health Record
EMR	Electronic Medical Record
HIAL	Health Information Access Layer
PHI	Private Health Information
SAML	Security Assertion Markup Language
SSL	Secure Sockets Layer
SSO	Single Sign-On
TLI	Transport Layer Interoperability
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

3.2 Definitions

The following are the terms and definitions used to describe the concepts used in this document.

TERM	DEFINITION
EHR Service	A service hosted on the provincial HIAL. Each EHR Service will have a unique target endpoint or URI within the EMR Offering.