EMR EHR Connectivity 2.0

Provincial Gateway – Requirements

December 23, 2019

Document Version & Status: 1.0 – DFC (Draft for Comment)

Table of Contents

1. INTRODUCTION 3

1.1 OVERVIEW 3
1.2 SCOPE 3
1.2.1 In Scope 3
1.2.2 Out of Scope 3
1.3 ASSUMPTIONS 3
1.4 DEPENDENCIES 3
1.5 RELATED DOCUMENTS, REFERENCES AND SOURCES 4

2. EMR REQUIREMENTS 5

2.1 EMR OFFERING (CLIENT) AUTHENTICATION 6
2.2 BUSINESS ORGANIZATION AND UAO 9
2.3 ERROR AND WARNING MANAGEMENT 12
2.4 LOGGING AND AUDITING 12

3. APPENDIX A: ADDITIONAL REFERENCES 14

DRAFT

1. INTRODUCTION

1.1 Overview

This document defines requirements and provides guidance to integrate functionality within an EMR Offering to connect to the Ontario Health ONE Access Provider Gateway (Provincial Gateway) to facilitate standardized access for EMR users to provincial EHR products and services through the use of the Open Authorization 2.0 (OAuth2) standard.

1.2 Scope

1.2.1 In Scope

- Functional requirements for an EMR Offering to be able to connect to the Provincial Gateway using OAuth2 with OIDC for identification, authentication and authorization.

1.2.2 Out of Scope

- Business processes to register an EMR for authorization to connectivity to the Provincial Gateway are managed by Ontario Health.
- Business processes to register an EMR or EMR user for authorization to access to an EHR product or service are managed by Ontario Health and the respective EHR product or service owner.
- Functional requirements for EMR Offerings to be able to connect to any specific EHR product or service is available in the respective EMR specification.

1.3 Assumptions

- The reader has a working knowledge of OAuth2, OIDC and HEART standards and protocols.
- The reader has a working knowledge of Application Programming Interfaces (APIs).

1.4 Dependencies

- The Provincial Gateway leverages ONE ID Identity Federation functionality for an EHR user to be able to successfully connect to an EHR service. As a result, implementation of the "Federation Identity and Single Sign-On" requirements of this EMR EHR Connectivity 2.0 Specification is needed to successfully authenticate the EMR user for access to an EHR service. Refer to the "Under the Authority of" (UAO) in the "ONE ID OAuth2/OpenID Specification" document for further details.
- Both an assigned X-Gtwy-ClientId and X-Gtwy-Client-Secret value are needed for a client application (e.g., EMR Offering) to interact with the Provincial Gateway in any (production or non-production) environment. The implementer will need to follow the Ontario Health registration processes to obtain

DRAFT

these values to connect to the Provincial Gateway. Refer to the "Client Application Registration" section of the "ONE Access Gateway" document for further details.

- The ONE Access Gateway leverages standard protocols for client applications (e.g., EMR Offerings) to communicate with it. As such, EMR Offerings need to align to these same standards to facilitate the interaction:
  - OAuth 2.0 (OAuth2)
  - OpenID Connect (OIDC) 1.0
  - Health Relationship Trust (HEART) for OpenID Connect 1.0

1.5 Related Documents, References and Sources

ID	NAME	VERSION	DATE
1	ONE Access Gateway – Transport Specification (Ontario Health, 2019) https://www.ehealthontario.on.ca/en/standards/view/one-access-gateway-transport-specification	0.1 Draft	2019-10-08
2	ONE ID OAuth2/OpenID Specification (Ontario Health, 2019) https://www.ehealthontario.on.ca/en/standards/view/one-id-openid-connect-specification	0.1 Draft	2019-10-08

DRAFT

2. EMR REQUIREMENTS

This section consists of the EMR functional requirements for interacting with the Provincial Gateway.

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 version
P = Previous requirement
U = Updated requirement from the previous EMR Specification version
R = Retired requirement from the 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 EMR Offering (Client) Authentication

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
IAA01.01	The EMR Offering MUST have a configurable field to store and use the Gateway Client ID.	The EMR Offering MUST be able to store and provide the Gateway Client ID to the Provincial Gateway to authenticate the EMR Offering. The EMR Offering MUST be able to store the Gateway Client ID. The EMR Offering MUST NOT be able to attempt connections to the Provincial Gateway without a populated Gateway Client ID value. The default value MUST be unpopulated. The ability to update the Gateway Client ID value within the EMR Offering MUST be restricted to specific (e.g., administrative) users. Changes made (add/update/delete) to the Gateway Client ID value MUST be logged for auditing purposes. Refer to the ONE ID OAuth2/OpenID Specification document and ONE Access Gateway – Transport Specification for details.	M	N
IAA01.02	The EMR Offering MUST have a configurable field to store and use the Gateway Client Secret.	The EMR Offering MUST be able to store and provide the Gateway Client Secret to the Provincial Gateway to authenticate the EMR Offering.	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		The EMR Offering MUST be able to store unique Gateway Client Secret values per EMR Offering instance. The EMR Offering MUST NOT be able to attempt connections to the Provincial Gateway without a populated Gateway Client Secret value. The default value MUST be unpopulated. The EMR Offering MUST treat the Gateway Client Secret as restricted information. The ability to update the Gateway Client Secret value within the EMR Offering MUST be restricted to specific (e.g., administrative) users. Changes made (add/update/delete) to the Gateway Client Secret value MUST be logged for auditing purposes. Refer to the ONE ID OAuth2/OpenID Specification document and ONE Access Gateway – Transport Specification for details.		
IAA01.03	The EMR Offering MUST have a configurable field to store and use the public key.	The public key is a Base64-encoded X.509 certificate. Refer to the ONE ID OAuth2/OpenID Specification document for details.	M	N
IAA01.04	The EMR Offering MUST have a configurable field for the Provincial Gateway endpoint value.	The EMR Offering MUST use the Gateway endpoint value (e.g., URI) to connect to the Provincial Gateway. The ability to update the Gateway endpoint value within the EMR Offering MUST be restricted to specific authorized users (e.g., administrative).	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Changes made (add/update/delete) to the Gateway endpoint value MUST be logged for auditing purposes. Refer to the ONE Access Gateway – Transport Specification for details.		
IAA01.05	The EMR Offering MUST have the ability to store and provide the X-LobTxId value.	The EMR Offering MUST have the functionality to store and provide the X-LobTxId value when required. Refer to the ONE Access Gateway – Transport Specification for details. **Note**: This requirement is optional for the functionality to connect but is mandatory when implementing an EHR service that requires this value. For example, the DHDR EHR service leverages a viewlet that requires the X-LobTxId value.	O	N

2.2 Business Organization and UAO

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
IAA02.01	The EMR Offering MUST have the functionality to maintain a list of EMR users' registered UAO values.	The EMR Offering MUST have an interface to allow an EMR user to manage (e.g., add, modify, delete) "Under the Authority of" (UAO) values assigned to each EMR user. The EMR Offering MUST restrict authorization to maintain UAO values to specific (e.g., administrative) EMR users. The EMR Offering MUST allow an EMR user to be associated with none, one or multiple UAO values. The EMR Offering MUST maintain the following data for each EMR user: a) EMR user b) UAO value(s) c) UAO organization name for each UAO value Refer to the "Under Authority of (UAO) Management" section of the ONEID OAuth2/OpenID Specification for more details. **Note**: An EMR user may be assigned zero, one or more UAO values.	M	N
IAA02.02	The EMR Offering MUST send the EMR user's business organization (UAO) when connecting to an EHR service.	The EMR Offering MUST automatically include the UAO identifier value if one exists when requesting access to an EHR service for the EMR user. Where the EMR user is not assigned any UAO value, then it MUST be omitted.	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
IAA02.03	The EMR Offering MUST have the ability to prompt the EMR user for their business organizations when authorizing access to an EHR service.	Where the EMR user has more than one assigned UAO value, then the EMR Offering MUST prompt the EMR user for a selection of all the possible UAO values to choose to include. The EMR Offering MUST NOT provide a selection to EMR users who have only one UAO value. The EMR Offering MUST continue with that one value as the UAO value (as if the EMR user selected the single option). At a minimum, the EMR Offering MUST display the following UAO attributes to the EMR user: a) Friendly name The EMR Offering MAY additionally display the following UAO attributes to the EMR user: b) Identifier c) Type	M	N
IAA02.04	The EMR Offering MUST provide the ability for an EMR user to manually change the UAO under which they are accessing an EHR service.	This function SHOULD only be available where the EMR user is assigned more than one UAO value. **Note**: The organization is identified by the UAO value. **Informational**: An EMR user may work on behalf of multiple HICs, where they need to identify and switch between the HICs when access EHR services. This functionality is pertinent when an EMR user is already connected to an EHR service as one UAO and needs to switch to a different UAO.	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
IAA02.05	The EMR Offering MUST maintain the UAO values for all EHR users in the EMR Offering.	EMR users may need to identify which organization(s) (i.e., UAO value) to send when connecting to an EHR service. The EMR Offering MUST have a means to maintain (e.g., store, provide, update) UAO values for each EHR user registered in the EMR Offering. The EMR Offering MUST: a) be able to support assigning zero or more UAO values to each EMR user registered in the EMR Offering b) be able to add and remove users to the table c) store the UAO value and attributes (e.g., the type of value, the value itself and the associated friendly name) d) present, at a minimum, the friendly name when prompting the EMR user to choose a UAO value. **Informational**: UAO values are provided as part of the Ontario Health registration process of an EMR user to obtain a federated identity (e.g., ONE ID account).	M	N

2.3 Error and Warning Management

Note: To consume EHR services, EMR Offerings will need to support application errors that are specific to the respective EHR product or service. These application errors are specific to each EHR product or service and are not defined in this section.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
IAA03.01	The EMR Offering MUST take appropriate actions for errors that can occur while communicating with the Provincial Gateway.	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 ONE Access Provider Gateway. 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 ONE Access Provider Gateway. **Unspecified errors**: Errors that occur when the ONE Access Provider Gateway experiences internal problems.	M	N

2.4 Logging and Auditing

EMR systems log various information and interactions and may contain private health information (PHI). As a result, consideration should be taken to log only what is necessary to avoid unintentionally saving or providing access to logged PHI and should be regarded with the same sensitivities as data containing PHI.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
IAA04.01	The EMR Offering MUST generate and provide the X-Request-Id value during all interactions with the Provincial Gateway.	The X-Request-Id value MUST be populated in the header of each transaction originating from the EMR Offering to the Provincial Gateway.	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		The X-Request-Id MUST be generated by the EMR Offering that is unique (to that EMR instance or assigned Client ID). The X-Request_Id values provided MUST be logged and accessible for view by the EMR user. Access MAY be restricted to specific EMR user(s). **Note**: The X-Request-Id is identified as optional for client applications. However, it is required for EMR Offerings to populate.		
IAA04.02	The EMR Offering MUST log successful and failed transactions with the Provincial Gateway and any EHR service.	At a minimum, the following information MUST be logged, if available a) EMR Offering transaction ID b) Date and time transaction initiated c) Gateway Client ID of the EMR system attempting the transaction d) The EMR user attempting the transaction, if applicable e) The EMR user's UAO used to attempt the transaction, if available f) Transaction attempted by the EMR user or system g) Status of the message (e.g., success or failure) h) Provincial Gateway response transaction ID i) EHR Service transaction ID j) System UAO, if available k) Target system (e.g., system name or EHR service name) Additional information SHOULD be logged within the EMR Offering, as necessary to facilitate troubleshooting and auditing. Refer to the "x-LobTxId" message header name of the Request Tracking section in the ONE Access Provider Gateway document.	M	N

3. APPENDIX A: ADDITIONAL REFERENCES

The following are supporting documentation and recommended reading.

ID	NAME	VERSION	DATE
1	EHR Connectivity Strategy (Ontario Health, 2019) https://www.ehealthontario.on.ca/en/ehr-connectivity-strategy	N/A	2019
2	Final: OpenID Connect Core 1.0 (The OpenID Foundation, 2014) https://openid.net/specs/openid-connect-core-1_0.html	N/A	2014
3	Health Relationship Trust Profile for OpenID Connect 1.0 (Richer, 2016) https://openid.net/specs/openid-heart-openid-connect-1_0-2017-05-31.html	N/A	2016-10-03
4	ONE ID Provincial Identity Federation Overview of SAML Configuration (Ontario Health, 2018)[1] https://www.ehealthontario.on.ca/en/standards/view/single-sign-on-patient-context-sharing-standard/	1.49 (1.4)	2017-08-21
5	RFC 6749 – The OAuth 2.0 Authorization Framework (Internet Engineering Task Force, 2012) https://tools.ietf.org/html/rfc6749	N/A	2012-10

[1] Version 1.5 of this document is published but does not apply and should not be referenced.