EMR EHR Connectivity 2.1

ONE Access Gateway – 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
1.3.2 Out of Scope 4
1.4 Assumptions 4
1.5 Dependencies 4
1.6 Related Documents, References and Sources 4

2. EMR REQUIREMENTS 6

2.1 EMR Offering (Client) Authentication 7
2.2 EHR Services 10
2.3 Error and Warning Management 12
2.4 Logging and Auditing 13

3. APPENDIX A: ADDITIONAL REFERENCES 15

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 (Digital Services) (OHDS) ONE Access Gateway (OAG) to facilitate standardized access for EMR users to provincial EHR products and services through the use of the Open Authorization 2.0 (OAuth2) standard and RESTful Fast Healthcare Interoperability Resources (FHIR) standards.

1.2 Version History

VERSION	REVISION DATE	REVISION NOTES
1.0	2019-12-23	a) The initial release of OAG requirements b) Added Readme document to identify SSO optionality
1.1	2020-07-13	a) Updated prefixes of OMD #s from "IAA" to "OAG", changed the title of the document to ONE Access Gateway (OAG) b) Changed all references of the Provincial Gateway to ONE Access Gateway c) Updated references to Ontario Health to Ontario Health (Digital Services), formerly eHealth Ontario d) Added reference to Ontario Health's EMR Integration with Viewlet Framework document to reference Provincial Gateway error codes e) Added section 2.2 (EHR Services) as new EHR Service section to support the ability to configure endpoints for each EHR Service f) Updated OAG01.03 noting public enrollment process g) Added OAG01.05 to reference session expiry and refresh from the OAG h) Added OAG01.06 to reflect token timeout periods i) Added OAG01.07 to reference adherence to OHDS specifications j) Updated OAG02.01 for user UAO values k) Added OAG02.06 to support organization UAO values l) Moved UAO to section 2.3 in the Federation ID and SSO requirements document m) Updated OAG03.01 to reference OAG error codes n) Added new OAG03.02 to address response timeout for APIs o) Updated OAG04.01 to reference the mandatory generation of a transaction ID to the OAG

1.3 Scope

1.3.1 In Scope

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

DRAFT

1.3.2 Out of Scope

- Business processes to register an EMR for authorization to connectivity to the OAG are managed by OHDS.
- Business processes to register an EMR or EMR user for authorization to access to an EHR product or service are managed by OHDS 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.

1.4 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).

1.5 Dependencies

- The OAG 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 2.1 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.
- Some information, such as the X-Gtwy-Client-Id and X-Gtwy-Client-Secret values are needed for a client application (e.g., EMR Offering) to interact with the OAG in a given environment. The implementer will need to follow the OHDS registration processes to obtain these values to connect to the OAG. Refer to the "Registration Activities" section of the ONE Access Gateway – Transport Specification 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

1.6 Related Documents, References and Sources

ID	NAME	VERSION	DATE
1	EMR Integration with Viewlet Framework – Developer Guide (Ontario Health Digital Services, 2019) Contact EMR@OntarioMD.com for the most current version available	0.9	2020-03-35
2	ONE Access Gateway – Transport Specification (Ontario Health Digital Services, 2020)	1.0	2020-01-09

ID	NAME	VERSION	DATE
	https://www.ehealthontario.on.ca/en/standards/view/one-access-gateway-transport-specification		
3	ONE ID OAuth2/OpenID Specification (Ontario Health Digital Services, 2020) https://www.ehealthontario.on.ca/en/standards/view/one-id-openid-connect-specification	1.0	2020-01-09

DRAFT

2. EMR REQUIREMENTS

This section consists of the EMR functional requirements for interacting with the One Access Gateway (OAG).

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
OAG01.01	The EMR Offering MUST adhere to OHDS requirements for the OAG.	The EMR MUST follow OAuth2.0 and OpenID standards as implemented by OHDS. Any requirements identified in both “ONE Access Gateway – Transport Specification” and “ONE ID OAuth2/OpenID Specification” documents must be adhered to. Refer to the Related Documents, References and Sources section for links to OHDS specifications.	M	P
OAG01.02	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 OAG 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 OAG without a populated Gateway Client ID value. The default value MUST be unpopulated (i.e., blank). The ability to update the Gateway Client ID value within the EMR Offering MUST be restricted to specific (e.g., administrative) user(s). Changes made (add/update/delete) to the Gateway Client ID value MUST be logged for auditing purposes.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Refer to the "ONE ID OAuth2/OpenID Specification" document and "ONE Access Gateway – Transport Specification" for more details on the Gateway Client ID.		
OAG01.03	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 OAG to authenticate the EMR Offering. 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 OAG 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 Audit and Logging section of this document for more information. Refer to the "ONE ID OAuth2/OpenID Specification" document and "ONE Access Gateway – Transport Specification" for more details on the Gateway Client Secret.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
OAG01.04	The EMR Offering MUST have a configurable field to store and use the public key.	Refer to the Interface Specifications section in the "ONE ID OAuth2/OpenID Specification" document for more information on keys. **Note**: The public key is provided as part of the enrollment process into the OAG.	M	P
OAG01.05	The EMR Offering MUST have a configurable field for the OAG endpoint value.	The EMR Offering MUST use the Gateway endpoint value (e.g., URI) to connect to the OAG. The ability to update the Gateway endpoint value within the EMR Offering MUST be restricted to specific authorized users (e.g., administrative). Changes made (add/update/delete) to the Gateway endpoint value MUST be logged for auditing purposes. Refer to the "ONE Access Gateway – Transport Specification" document for more details on OAG endpoints. **Note**: Endpoints may be referred to as Base Gateway Endpoint in the ONE Access Gateway – Transport Specification document.	M	P
OAG01.06	The EMR Offering MUST have the functionality to detect time out periods and notify the EMR user before the session expires.	The EMR Offering MUST be able to detect all time out periods from the OAG. Where a session refresh is possible the EMR Offering MUST be able to allow the EMR user with the option to refresh the session. Refer to the "ONEID OAuth2/ OpenID Specification" document for more information on implementation, specifications, policies, and validity periods of tokens.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Any EMR Offering timeouts MUST NOT conflict with the timeout periods of the gateway. **Note**: Token validity periods are defined by OAuth2.		

2.2 EHR Services

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
OAG02.01	The EMR Offering MUST extract and use endpoint values to interact with EHR Services.	As part of the login process to the OAG, the EMR Offering MUST request endpoint values used to interact with EHR Services. For each EHR Service available, the EMR Offering MUST use the configured EHR endpoint value to connect to the respective EHR Service. Any endpoint values provided in tokens should not be hardcoded. Refer to hub.url in the "EMR Integration with Viewlet Framework" document for more information on endpoint extracting endpoint values for EHR Services.	M	P
OAG02.02	The EMR Offering MUST have a configurable field to identify each supported EHR Service.	For each EHR Service available, the EMR Offering MUST maintain the following information. a) EHR Service Name b) EHR Service Version c) EHR endpoint d) API Key The EMR Offering MUST be able to support the ability to have different versions of an EHR Service to be deployed in clinical practices.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		The EHR endpoint MUST be configurable. The EMR Offering MUST restrict access to modify the EHR endpoint value to specific EMR user(s) or EMR vendor support staff. The above information MUST exist for every EHR service hosted on the OAG that is supported by the EMR Offering. The EHR Service Name and EHR Service Version are informational labels to identify the EHR Service and provide no other functional purpose. Refer to the OAG Transport Specification for more information regarding the API Key.		
OAG02.03	EHR Service API Key MUST be configurable for each supported EHR Service.	For each EHR Service available, the EMR Offering MUST use the configured EHR Service API Key value when calling an API to the respective EHR Service. It is not acceptable to hard code the EHR Service API Key value.	M	P
OAG02.04	The OAG response wait time MUST be assigned an initial value within the EMR Offering.	The response wait time is defined by the OAG and MUST have an initial value pre-set three hundred (300) seconds.	M	N
OAG02.05	The OAG response wait time MUST be configurable within the EMR Offering interface.	The OAG response wait time may change in the future and MUST be a configurable value within the EMR Offering. The value SHOULD represent a unit of time in seconds.	M	N

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		The OAG response time MUST be restricted and allowed to be changed only by authorized staff (e.g., super EMR user, or EMR vendor support staff).		

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
OAG03.01	The EMR Offering MUST take appropriate actions for gateway responses while communicating with the OAG.	At a minimum, the EMR Offering MUST identify gateway response codes and notify the EMR user where any errors occur. Where an EMR Offering encounters an error while communicating with the OAG, the EMR Offering MUST take appropriate actions to resolve the errors. Refer to the "Gateway Response Codes" in the "ONE Access Gateway – Transport Specification" document for details on gateway responses.	M	P
OAG03.02	The EMR Offering MUST be able to handle timeout errors where no error response is returned from the OAG.	The EMR Offering MUST wait for an expected response from the Provider Gateway (including transactions with the EHR service) for a period up to the Provider Gateway Timeout Period. The EMR Offering MUST provide a warning message if an expected response from the Provider Gateway (including transactions with the EHR service) is not received within the Gateway Timeout Period. **Note**: The OAG Timeout Period is currently set to five (5) minutes by the OAG.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Informational: The OAG Timeout Period is a timeout when an expected response is not received from the EMR Offering to the OAG. This timeout applies to communications with the OAG, to any EHR Service, the Context Management System, and any Viewlet.		

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
OAG04.01	The EMR Offering MUST generate and provide a transaction ID (X-Request-Id) value during all interactions with the OAG.	The X-Request-Id value MUST be populated in the header of each transaction originating from the EMR Offering to the OAG. 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.	M	P
OAG04.02	The EMR Offering MUST log successful and failed transactions with the OAG and any EHR service.	At a minimum, the following information MUST be logged, if available a) EMR Offering transaction ID (X-Request-Id) b) Date and time transaction initiated	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		c) Gateway Client ID (X-Gtwy-Client-Id) of the EMR system attempting the transaction d) The EMR user attempting the transaction, if applicable e) Action or request attempted by the EMR user or system f) Status of the message (e.g., success or failure) g) OAG response transaction ID (X-Correlation-Id) h) Target system (e.g., system name or EHR service name) i) Line of Business transaction ID (X-LobTxId, if available) Additional information SHOULD be logged within the EMR Offering, as necessary to facilitate troubleshooting and auditing. Refer "ONE Access Gateway – Transport Specifications" document for more information on logging parameters provided by OAG.		

3. APPENDIX A: ADDITIONAL REFERENCES

The following are supporting documentation and recommended reading.

ID	NAME	VERSION	DATE
1	EHR Connectivity Strategy (Ontario Health Digital Services, 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 Digital Services, 2018)[1] https://www.ehealthontario.on.ca/en/standards/view/single-sign-on-patient-context-sharing-standard/	1.5	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.