EMR EHR Connectivity

ONE Access Gateway – Requirements

May 21, 2021

Document Version & Status: 2.2 – DFU (Draft for Use)

Table of Contents

1. INTRODUCTION 3

1.1 OVERVIEW 3
1.2 VERSION HISTORY 3
1.3 SCOPE 4
1.3.1 In Scope 4
1.3.2 Out of Scope 4
1.4 ASSUMPTIONS 4
1.5 DEPENDENCIES 4
1.6 RELATED DOCUMENTS, REFERENCES AND SOURCES 5

2. EMR REQUIREMENTS 6

2.1 EMR OFFERING (CLIENT) AUTHENTICATION 7
2.2 EHR SERVICES 9
2.3 ERROR AND WARNING MANAGEMENT 11
2.4 LOGGING AND AUDITING 12

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 a 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.
1.2	2020-07-28	a) Updated reference to EMR Integration with Viewlet Framework from 0.9 to 0.10. b) Updated reference to ONE ID OAuth2/OpenID Specification from version 1.0 to 1.2. c) Updated reference to ONE ID Provincial Identity Federation Overview of SAML Configuration document from version 1.5 which is no longer used, to version 1.49. d) Removed Additional References and its references.
2.0	2020-12-09	a) Updated reference to ONE Access Viewlet Framework, which is now accessible online. b) Updated reference to Ontario Context Management System.

VERSION	REVISION DATE	REVISION NOTES
		c) Updated OAG02.01 for extraction and use of PCOI endpoint values. This functionality existed in Viewlet Framework requirements.
2.1	2021-03-04	a) Retired content and requirement to support the provincial HIAL gateway. b) Updated reference to ONE Access Viewlet Framework – Developer Guide (version, URL). c) Updated reference to ONE Access Gateway – Transport Specification (URL). d) Updated reference to ONE ID OAuth2/OpenID Specification (URL). e) New connections to the Health Information Access Layer (HIAL) using the Security Assertion Markup Language (SAML) are no longer accepted. As such, related content and requirements have now been retired.
2.2	2021-04-08	Updated reference to ONE Access Viewlet Framework (version).
2.2	2021-05-21	EMR Specification released as Draft for Use (DFU).

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 OpenID Connect (OIDC) for identification, authentication, and authorization.

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 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 are available in the respective EMR specification.

1.4 Assumptions

- The reader has a working knowledge of OAuth2, OIDC, and HEART (Health Relationship Trust Profile) 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 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 OAG 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	ONE Access Viewlet Framework – Developer Guide (Ontario Health Digital Services, 2021) https://ehealthontario.on.ca/en/standards/one-access-viewlet-framework-developer-guide	1.7	2021-03
2	ONE Access Gateway – Transport Specification (Ontario Health Digital Services, 2020) https://ehealthontario.on.ca/en/standards/one-access-gateway-transport-specification	1.0	2020-01-09
3	ONE ID OAuth2/OpenID Specification (Ontario Health Digital Services, 2020) https://ehealthontario.on.ca/en/standards/one-id-openid-connect-specification	1.2	2020-05-20

2. EMR REQUIREMENTS

This section consists of the EMR functional requirements for interacting with the 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

The following EMR requirements apply to functionality specific to 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 and requirements as identified in both documents: a) ONE Access Gateway – Transport Specification, and b) ONE ID OAuth2/OpenID Specification 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
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.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Note: The public key is provided as part of the enrollment process into the OAG.		
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. Any EMR Offering timeouts MUST NOT conflict with the timeout periods of the gateway. **Note**: Token validity periods are defined by OAuth2.	M	P

2.2 EHR Services

The following EMR requirements apply to functionality specific to EHR services connecting to the OAG.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
OAG02.01	The EMR Offering MUST retrieve the FHIR issuer endpoint value from the OAuth2 token request return in order to interact with the OAG.	It is not acceptable to hard code the FHIR issuer endpoint value in the EMR Offering. The FHIR issuer key – used to retrieve the FHIR issuer endpoint value – is found in the toolbar parameter in the OAuth2 token request return. Refer to “FHIR issue endpoint” and “FHIR_iss” in the Generic Use Case section of the ONE Access Viewlet Framework document for more information to identify the appropriate key and how to retrieve the FHIR issuer endpoint value. **Note**: The toolbar parameter contains additional parameters for other purposes.	M	U
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. 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.	M	P

		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	P
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. 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).	M	P

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	At a minimum, the EMR Offering MUST identify gateway response codes and notify the EMR user where any errors occur.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	responses while communicating with the OAG.	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.		
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. **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, or a Viewlet.	M	P

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. The following EMR requirements apply to functionality specific to logging and auditing for the OAG and are supplementary to the requirements identified in the Primary Care Baseline Specification.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
OAG04.01	The EMR Offering MUST generate and provide a transaction ID (X-Request-Id)	The X-Request-Id value MUST be populated in the header of each transaction originating from the EMR Offering to the OAG.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	value during all interactions with 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.		
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 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.	M	P