

EMR EHR Connectivity

ONE Access Gateway – Requirements

June 30, 2024

Document Version & Status: 2.3 – Final



Table of Contents

1. INTRODUCTION	3
1.1 OVERVIEW	3
1.2 VERSION HISTORY	3
1.3 SCOPE	4
1.3.1 <i>In Scope</i>	4
1.3.2 <i>Out of Scope</i>	4
1.4 ASSUMPTIONS	5
1.5 DEPENDENCIES	5
1.6 RELATED DOCUMENTS, REFERENCES AND SOURCES	5
2. EMR REQUIREMENTS	6
2.1 CLIENT APPLICATION AUTHENTICATION	7
2.2 EHR SERVICES	9
2.3 ERROR AND WARNING MANAGEMENT	10
2.4 LOGGING AND AUDITING	11

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 (OH) ONE Access Gateway (OAG) to facilitate standardized access for 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) Initial release b) Added Readme document to identify SSO optionality
1.1	2020-07-13	a) Updated prefixes of OMD #s from “IAA” to “OAG”, and 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 the 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 c) Updated OAG02.01 for extraction and use of PCOI endpoint values. This functionality existed in the Viewlet Framework requirements

VERSION	REVISION DATE	REVISION NOTES
2.1	2021-03-04	a) Retired content and requirements 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	2021-04-09	Updated reference to ONE Access Viewlet Framework (version)
2.2	2021-05-21	EMR Specification released as Draft for Use (DFU)
2.2	2021-05-31	EMR Specification released as Final
2.3	2024-06-30	a) Various errata and format corrections b) Updated OAG01.03 retiring references to client secret and replaced with Public Key Infrastructure (PKI) certificates. c) Retired OAG01.01, it is implied d) Updated OAG01.02 for clarity e) Updated OAG01.04 for clarity f) Retired OAG01.05, no longer relevant g) Re-sequenced OAG01.05, was previously OAG01.06 h) Updated OAG01.06 for clarity around refreshing OAuth2 tokens i) Updated OAG02.01 for clarity on the use of parameter values to interact with the OAG j) Updated OAG02.02, retired API key from guidelines k) Retired OAG02.04 and OAG02.05 values for timeouts are Defined by OH l) Updated OAG03.02 for clarity on when to provide error messages m) Updated OAG04.01 for clarity on references to the X-Request-ID

1.3 Scope

1.3.1 In Scope

- Functional requirements 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 connect to the OAG are managed by OHDS.
- Business processes to register an EMR or user for authorization to access an EHR product or service managed by OHDS and the respective EHR product or service owner.

Note: 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 ONEID Identity Federation functionality for a 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 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 value is 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 OH 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, 2022) https://ehealthontario.on.ca/en/standards/one-id-openid-connect-specification	1.6	2022-08-18

2. EMR REQUIREMENTS

This section consists of the functional requirements for interacting with the OAG.

Support:

M = Mandatory. EMR Offerings certified for this specification **MUST** support this requirement.
O = Optional. Vendors **MAY** choose to support this requirement in their certified EMR Offering.

Status:

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

OMD #:

A unique identifier that identifies each requirement within OMD's EMR Specifications 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 contain additional instructions or detail about the high-level requirement. The text in both columns is considered requirement statements.

2.1 Client Application 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 OH requirements for the OAG.	The EMR MUST follow OAuth2.0 and OpenID standards and requirements as identified in both the following documents. a) ONE Access Gateway – Transport Specification b) ONE ID OAuth2/OpenID Specification	M	R
OAG01.02	The EMR Offering MUST have a configurable field to store and provide the Client ID when authenticating the EMR Offering.	The EMR Offering MUST NOT be able to attempt connections to the OAG without a populated Client ID value. The default value MUST be unpopulated (i.e., blank). The ability to update the Client ID value within the EMR Offering MUST be restricted to specific privileged users (e.g., administrators). Changes made (add/update/delete) to the 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 more details on the Client ID. Note: The Client ID is assigned by OH per EMR installation (e.g., to each clinic facility).	M	U
OAG01.03	The EMR Offering MUST have the functionality to store and use the Public	The PKI certificate is used to generate a client assertion as part of the token request process.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	Key Infrastructure (PKI) certificate for token requests.	The EMR Offering MUST be able to store a unique PKI Certificate per EMR Offering instance. The EMR Offering MUST NOT proceed with attempts to connect to the OAuth2 server without a populated PKI certificate value. The EMR Offering MUST treat the PKI certificate as restricted information. The ability to update the PKI certificate value within the EMR Offering MUST be restricted to specific (e.g., administrative) users. Changes made (add/update/delete) to the PKI certificate 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 PKI certificate.		
OAG01.04	The EMR Offering MUST have a configurable field to store and use the OAG’s 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 OH’s OAG enrollment process.	M	U
OAG01.05	The EMR Offering MUST have the functionality to automatically maintain active OAuth2 tokens.	The EMR Offering MUST be able to store active OAuth2 tokens and take appropriate action to refresh tokens when they expire. The EMR Offering MUST be able to detect token expiry periods in the token.	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Refer to the “ONEID OAuth2/OpenID Specification” document for more information on the implementation, specifications, policies, and validity periods of tokens. Note: Token validity periods are defined by OAuth2.		

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 and utilize parameter values from the OAuth2 token request return to interact with EHR services.	It is not acceptable to hard code the parameter endpoint values in the EMR Offering. Refer to “toolbar (Base64 encoded) parameters” in the “ONE Access Viewlet Framework Developer Guide” for more information on toolbar parameters.	M	U
OAG02.02	The EMR Offering MUST have configurable fields to identify each supported EHR Service.	The EMR Offering MUST maintain the following configurable information for each EHR Service that is supported by the EMR Offering: a) EHR Service Name b) EHR endpoint value The EMR Offering MUST restrict access to modify the configurable fields for each EHR Service to specific users or EMR vendor support staff. The EHR Service Name is an informational label to identify the EHR Service and is useful when more than one EHR Service is configured.	M	U

OAG02.03	The EMR Offering MUST align with the timeout period defined by the OAG.	The OAG Timeout Period is defined by OH. EMR Offering timeout period for interacting with the OAG MUST align to the timeout period defined by the OAG.	M	U
----------	---	---	---	---

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 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 defined by the OAG Timeout Period. Where no error response is returned from the OAG, the EMR Offering MUST provide a warning message to the user if an expected response from the Provider Gateway (including transactions with the EHR service) is not received within the period defined by the OAG Timeout period. 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	U

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 unique transaction ID (X-Request-Id) value for every interaction 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 and is unique to each transaction initiated by the EMR Offering. The X-Request-Id values provided MUST be logged and accessible for viewing by the user. Access MAY be restricted to specific user(s). Refer to the “ONE Access Gateway – Transport Specification” and “ONE Access Gateway – Requirements” documents for more details on the X-Request-Id. Important: The X-Request-ID is needed for interactions with CMS	M	U
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) Client ID (X-Gtwy-Client-Id) of the EMR system attempting the transaction d) The user attempting the transaction, if applicable e) Action or request attempted by the 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 MUST be logged within the EMR Offering, as necessary to facilitate troubleshooting and auditing.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Refer "ONE Access Gateway – Transport Specifications" document for more information on logging parameters provided by OAG.		