

# EMR EHR Connectivity

## Federation Identity and Single Sign-On – Requirements

June 30, 2024

Document Version & Status: 2.3 – Final



## Table of Contents

<b>TABLE OF CONTENTS .....</b>	<b>2</b>
<b>1. INTRODUCTION .....</b>	<b>3</b>
1.1 RELATED DOCUMENTS, REFERENCES, AND SOURCES.....	3
1.2 VERSION HISTORY.....	3
1.3 SINGLE SIGN-ON (SSO) AND BINDING .....	4
<b>2. EMR REQUIREMENTS .....</b>	<b>5</b>
2.1 EMR LOGIN .....	6
2.2 EMR BINDING TO FEDERATED IDENTITY.....	8
2.3 UNDER THE AUTHORITY OF (UAO) VALUES.....	9
2.4 LOG OUT .....	12
2.5 ERROR HANDLING.....	13
2.6 LOGGING AND AUDITING.....	13

## 1. INTRODUCTION

The purpose of this document is to provide implementers with functional requirements and guidance to integrate Digital Services Identity Federation and Sing Sign-On functionality within an EMR Offering to access provincial Electronic Health Record (EHR) products and services. Single Sign-On is when a user is authenticated with ONE ID, the authentication is used to gain access to ALL EHR assets to which the user is entitled.

### 1.1 Related Documents, References, and Sources

ID	NAME	VERSION	DATE
1	ONE ID OAuth2/OpenID Specification (Ontario Health, 2022) <a href="https://ehealthontario.on.ca/en/standards/one-id-openid-connect-specification">https://ehealthontario.on.ca/en/standards/one-id-openid-connect-specification</a>	1.6	2022-08-18

### 1.2 Version History

VERSION	REVISION DATE	REVISION NOTES
1.0	2019-12-23	Initial release
1.1	2020-07-13	<ul style="list-style-type: none"> <li>a) Updated SSO01.02 to log the EMR user into the EMR Offering using SSO.</li> <li>b) Added SSO01.04 to include functional parity between EMR login credentials and SSO login credentials.</li> <li>c) Added SSO01.05 to allow for EHR Service visibility to be configurable.</li> <li>d) Added UAO section into requirements (previously in OAG requirements).</li> <li>e) Added SSO04.02 to allow for UAO error notification.</li> <li>f) Added SSO05.03 for auditing and logging UAO.</li> </ul>
2.0	2020-12-09	<ul style="list-style-type: none"> <li>a) Removed example token files from the Specification package.</li> <li>b) Inserted SSO and SSO binding optionality instructions for implementers.</li> <li>c) Updated SSO04.03 to separate requirements around removing exposure to PHI when an EMR user logs out (into SSO04.04).</li> <li>d) Added SSO04.04 to move out PHI-related requirements from SSO04.03 and to include alternative options where an EMR cannot control the display of PHI.</li> <li>e) Re-numbered original SSO04.04, now SSO04.05.</li> </ul>
2.1	2021-03-04	<ul style="list-style-type: none"> <li>a) Updated reference to ONE ID OAuth2/OpenID Specification</li> <li>b) 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.</li> <li>c) Updated SSO01.05 to provide clarity to differentiate access control within and outside of the EMR.</li> </ul>

VERSION	REVISION DATE	REVISION NOTES
2.1	2021-05-21	EMR Specification released as Draft for Use (DFU).
2.1	2021-05-31	EMR Specification released as Final.
2.2	2024-06-30	<ul style="list-style-type: none"> <li>a) "EMR user" is replaced with "user" in all requirements and guidelines where applicable.</li> <li>b) Updated errata and format corrections.</li> <li>c) Retired SSO01.02, merged with SSO01.01</li> <li>d) Updated SSO01.04 for clarity allowing user choice to bind IDP credentials</li> <li>e) Updated SSO02.01 for clarity on binding local EMR credentials and Federated IDs</li> <li>f) Renumbered SSO02.03 to SSO01.06</li> <li>g) Renumbered SSO02.04 to SSO01.07</li> <li>h) Updated SSO03.01 for clarity on UAO values coming from the EMR Offering, not the OH UAO picker.</li> <li>i) Updated SSO03.02 to remove UAO value types, no longer needed for UAO.</li> <li>j) Updated SSO03.03 for clarity on the selection of UAO values from within the EMR Offering.</li> <li>k) Updated SSO03.04 for clarity on limiting interactions with the Authentication Server and OAG without a UAO value.</li> <li>l) Updated SSO03.05 for clarity on EMR users switching UAO values.</li> <li>m) Updated SSO04.01 for clarity regarding the IDP timeout period</li> <li>n) Re-sequenced the following requirements: <ul style="list-style-type: none"> <li>I. SSO04.01, was previously SSO04.03</li> <li>II. SSO04.02, was previously SSO04.04</li> </ul> </li> <li>o) Updated SSO04.01 for clarity, previously stated "all SSO sessions", now states "any SSO session" implying that there is no expectation to support multiple SSO sessions.</li> <li>p) Retired SSO04.05, functionality not relevant for SSO.</li> <li>q) Retired SSO05.02, merged with SSO05.01.</li> </ul>

### 1.3 Single Sign-On (SSO) and Binding

Functionality related to associating (binding) EMR credentials and Federated IDP credentials in this document is **OPTIONAL** for implementation. Note that proceeding with the binding functionality requires the implementation of all SSO and SSO binding requirements in full – a partial implementation is not adequate.

The following list identifies OMD #s of the specific EMR requirements that relate to the binding. Refer to the EMR requirements for implementation guidelines.

- SSO01.01
- SSO01.03
- SSO02.01
- SSO02.02

## 2. EMR REQUIREMENTS

This section consists of the EMR functional requirements for ID Federation and SSO.

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 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 contain additional instructions or detail about the high-level requirement. The text in both columns is considered a requirement statement.

## 2.1 EMR Login

The following EMR requirements apply to EMR functionality specific to EMR login with federated identity and SSO.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO01.01	The EMR Offering MUST present users with the option to log into the EMR Offering using credentials provisioned by the EMR Offering or their trusted Identity Provider (IDP) credentials.	<p>The EMR Offering MUST initiate the OAuth2 token workflow for the user to the Federated Identity Broker if the EMR user chooses to log in using their trusted IDP credentials.</p> <p>Once successfully authenticated by a trusted IDP at login, the EMR Offering MUST attempt authentication to respective EHR Services that leverage the IDP (i.e., without needing the user to enter EMR credentials) and for which the user has access.</p> <p>The EMR Offering MUST ONLY allow an IDP login where the user is already bound to the EMR Offering.</p>	M	U
SSO01.02	The EMR Offering MUST allow users to log into the EMR Offering using a Federated Identity user account.	Once successfully authenticated by a trusted IDP via the Federated Identity Broker, users MUST be automatically logged into the EMR Offering (i.e., without needing to enter EMR credentials).	M	R
SSO01.03	The EMR Offering MUST provide the user with the option to log in using only credentials provisioned by the EMR Offering.	If federated credentials are not needed by the user, or if the federated service is unavailable, the user MUST still be able to log into the EMR Offering.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO01.04	The EMR Offering MUST present the user with the same EMR functionality whether logging in with their EMR credentials or their trusted IDP credentials.	<p>Where a user logs in using their EMR credentials, the EMR Offering MUST NOT limit or remove the ability for a user to initiate launching EHR Services that they are authorized to use. The user MUST be prompted to log in using their trusted IDP credentials before being able to gain access to EHR Services where the user has not already authenticated using their IDP credentials (e.g., when logging into the EMR Offering).</p> <p>A user logged in with their EMR credentials wishing to launch an EHR Service MUST be prompted to enter their trusted IDP credentials without logging out of their session.</p>	M	U
SSO01.05	The EMR Offering MUST have the functionality to manage user access to EHR services within the EMR Offering.	<p>Access to EHR services SHOULD be configurable via a user interface.</p> <p>The ability to configure access to EHR Services within the EMR Offering MUST be restricted to specific (e.g., administrative) users.</p> <p><b>Note:</b> Access management by the EMR Offering provides another level of security, separate from access granted by the owner of an EHR Service.</p>	O	U
SSO01.06	The EMR Offering MUST NOT store or cache any user credentials for IDPs.	<p>The IDP user name and password, where required, MUST be provided by the EMR user.</p> <p>SSO to the EMR Offering and EHR services only occurs if the user has been successfully authenticated by a Federated Identity Provider via the Federated Identity Broker.</p>	M	U
SSO01.07	The EMR Offering MUST receive and store the IDP login session information for the duration of the user's login session.	Upon successful authentication of the user, the Provincial Federated Identity Broker service will return IDP login session information for the user to the EMR Offering to store during the user's login session.	M	U

## 2.2 EMR Binding to Federated Identity

The following EMR requirements apply to EMR functionality specific to EMR binding to a federated IDP.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO02.01	The EMR Offering MUST have the functionality to allow the user to associate (bind) their EMR credentials to their federated IDP credentials.	<p>The EMR Offering MUST bind the Federated IDP credentials with the requesting user's account, once both credentials have been authenticated. An association MUST be persistent and not require the binding to be re-established after the user logs out of the EMR Offering.</p> <p>The "Sub" OAuth2 attribute within the ID Token MUST be used to bind the Federated IDP credentials to the respective user account.</p> <p>A process that requires users to expose credentials to others (e.g., administrative users and vendor support staff) to facilitate the binding of credentials is not acceptable.</p> <p><b>Note:</b> The binding of a Federated SSO Identity with an EMR account allows a user to log into the EMR system using either credential (but only access EHR services if authenticated using their Federated SSO Identity).</p>	M	U
SSO02.02	The EMR Offering MUST provide the ability to disassociate (unbind) a Federated SSO Identity from the EMR user account.	The functionality to disassociate the EMR credentials from the IDP credentials MUST be available through the EMR user interface and not require assistance from the EMR Vendor support staff.	M	U

### 2.3 Under the Authority Of (UAO) Values

The following EMR requirements apply to federated identity and SSO EMR functionality specific to UAO values.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO03.01	The EMR Offering MUST have a configurable functionality to maintain a list of UAO values.	<p>The EMR Offering MUST have an interface to allow a user to manage (e.g., add, modify, delete) UAO values.</p> <p>The EMR Offering MUST restrict authorization to maintain UAO values to specific (e.g., administrative) users.</p> <p>At a minimum, the EMR Offering MUST maintain the following information for UAO values:</p> <ul style="list-style-type: none"> <li>a) UAO values</li> <li>b) UAO friendly names</li> </ul> <p>Refer to the “Under Authority of (UAO) Management” section of the ONEID OAuth2/OpenID Specification for more details.</p> <p><b>Note:</b> Ontario Health (OH) has created a UAO picker functionality, however, the EMR Offering MUST utilize UAO functionality from within the EMR Offering. Leveraging the OH UAO Picker is not an acceptable implementation.</p>	M	U
SSO03.02	The EMR Offering MUST allow users to be associated with UAO values.	The user may need to identify which 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 user registered in the EMR Offering.	M	U

		<p>At a minimum, the EMR Offering MUST:</p> <ul style="list-style-type: none"> <li>a) Be able to support assigning zero, one, or multiple UAO values to each user registered in the EMR Offering</li> <li>b) Be able to add and remove users to the list of UAO values.</li> </ul> <p>The EMR Offering MUST restrict the association of UAO values to specific (e.g., administrative) users.</p> <p><b>Informational:</b> UAO values are provided as part of the OH registration process of a user to obtain a federated identity (e.g., ONE ID account).</p>		
SSO03.03	<p>The EMR Offering MUST have the functionality to prompt the user to select a UAO value when logging into the EMR Offering.</p>	<p>Once the user is authenticated, the EMR Offering MUST prompt the user to select a UAO value assigned to them from the configured UAO values in the EMR Offering.</p> <p>Where the user has no assigned UAO value, the EMR Offering MUST NOT pre-select a default value for the user. The EMR Offering MUST continue with no assigned UAO value.</p> <p>Where the user has only one assigned UAO value, the EMR Offering MUST NOT provide a selection to the user. The EMR Offering MUST continue with the one assigned value in the EMR Offering as the UAO value (as if the user selected the single option).</p> <p>Where the user has more than one assigned UAO value, the EMR Offering MUST prompt the user for a selection of all the possible UAO values assigned to them in the EMR Offering.</p>	M	U

		<p>At a minimum, the EMR Offering MUST display the UAO-friendly name to the user.</p> <p>The EMR Offering MAY additionally display the UAO identifier attribute to the user.</p>		
SSO03.04	The EMR Offering MUST use the users assigned or selected UAO value for interactions and requests to the OAG.	<p>Where a user has an assigned or selected UAO value, the EMR Offering MUST automatically include the UAO value of the user to the OAG when requesting access to an EHR service.</p> <p>Where the user has no assigned or selected UAO value, The EMR Offering MUST NOT attempt to interact with the Authentication Server or the OAG.</p> <p>The EMR Offering MUST submit the scope of permissions as part of the authorization request for interactions with the OAG before using the UAO value to interact with the OAG.</p> <p>Refer to the “OpenID” scope in the ONEID OAuth2/OpenID Specification for more details on scopes.</p>	M	U
SSO03.05	The EMR Offering MUST have the functionality to allow a user to switch UAO values within their login session.	<p>The EMR Offering MUST prompt the user to select only from their assigned UAO values in the EMR Offering.</p> <p>Switching UAO values MUST only be available where the user is assigned multiple UAO values in the EMR Offering.</p> <p>Where the user wishes to switch their UAO, the EMR Offering MUST NOT prompt the user to log out of their session.</p>	M	U

		<p>At a minimum, the EMR Offering MUST display the friendly name associated with the UAO value to the user.</p> <p><b>Note:</b> A user may work on behalf of multiple HICs, where they need to identify and switch between the HICs when accessing EHR Services. This functionality is pertinent when a user is already connected to an EHR Service as one UAO and needs to switch to a different UAO.</p>		
--	--	--	--	--

## 2.4 Log out

The following EMR requirements apply to EMR functionality for logging out.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO04.01	The EMR Offering MUST gracefully end any active SSO session when the user logs out of the EMR Offering.	Refer to the “End Session Endpoint” section of the ONEID OAuth2/OpenID Specification for more details.	M	U
SSO04.02	The EMR Offering MUST mitigate any potential unauthorized exposure of PHI when the user logs out of the EMR Offering.	<p>When a user logs out of the EMR Offering, the EMR Offering MUST prevent the possible display of, and ability to modify PHI, when the user logs out of the EMR Offering, where possible (e.g., closing of browser windows).</p> <p>Only where it is not possible for the EMR Offering to prevent the potential display of PHI (e.g., on an external browser window), the EMR Offering MUST alternatively notify the user of the potential risk of unauthorized exposure of PHI and instructions to mitigate that risk.</p>	M	P

## 2.5 Error Handling

The following EMR requirements apply to EMR functionality specific to error handling with federated identity and SSO.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO05.01	The EMR Offering MUST take appropriate actions for all errors that can occur while communicating with a Federated Identity Broker.	<p>Where a user encounters an error while attempting to authenticate, the EMR Offering MUST notify the user of the error.</p> <p>The EMR Offering MUST log the errors and notify the user of the error as well as the appropriate next step(s) for the user.</p> <p>Refer to the ONEID OAuth2/OpenID Specification for more details on errors.</p>	M	U
SSO05.02	The EMR Offering MUST notify the user when any SSO error occurs.	<p>Where a user encounters an error while attempting to authenticate, the EMR Offering MUST notify the user of the error.</p> <p>Refer to the ONEID OAuth2/OpenID Specification for more details on errors.</p>	M	R

## 2.6 Logging and Auditing

EMR systems log different information and interactions. In some instances, PHI may be passed as parameters in 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. The following EMR requirements apply to functionality specific to logging and auditing for federated identity and SSO, they are supplementary to the requirements identified in the Primary Care Baseline Specification.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO06.01	The EMR Offering MUST log IDP login attempts to facilitate auditing and troubleshooting.	All (successful and failed) login attempts MUST be logged, where possible.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		<p>Additional information MUST be logged, as necessary and available, to facilitate auditing and troubleshooting processes.</p> <p>It is recommended to provide access to logs via the user interface.</p>		
SS006.02	<p>The EMR Offering MUST log errors generated by a Federated SSO Identity Broker.</p>	<p>At a minimum, the following MUST be logged:</p> <ul style="list-style-type: none"> <li>a) Action or request attempted by the user.</li> <li>b) The user who is attempting the action or request.</li> <li>c) Date and time the action and error occurred.</li> </ul> <p>It is recommended to provide access to logs via the user interface.</p>	M	P
SSO06.03	<p>The EMR Offering MUST log all transactions associated with UAO assignments.</p>	<p>The EMR Offering MUST be able to keep logs of all transactions for UAO assignments within the EMR Offering.</p> <p>At a minimum, it MUST capture:</p> <ul style="list-style-type: none"> <li>a) Which user made changes to any UAO assignments</li> <li>b) Which users had their UAO values changed?</li> <li>c) What changes were made to the assignment of UAO values?</li> <li>d) Date and time when changes were made to the assignment of UAO values.</li> <li>e) Previous condition of the UAO assignment</li> </ul> <p><b>Note:</b> Refer to each EHR service specification document for their use of system UAO values.</p>	M	P