RIAYATI Program

Single Sign-On (SSO) Integration

Document ID: **RYT-HIE-ICD-SSO-012**

Date: 26 May 2021 (v2)

UNITED ARAB EMIRATES
MINISTRY OF HEALTH & PREVENTION

Table of Contents

Version and Distribution History			
Version #	**Date**	**Brief Comments on Change**	**Author**
1.0	2-March-2021	Draft Specification	MOHAP
1.0	2-March-2021	Review	MOHAP
1.1	7-March-2021	Revised version	MOHAP
1.1	8-March-2021	Review	MOHAP
1.2	10-March-2021	Revised version	MOHAP
1.3	12-March-2021	Revised version	MOHAP
1.4	26-May-2021	Amendment for Record Indicator API	MOHAP
1.4	26-May-2021	Review Record Indicator	MOHAP
1.5	26-May-2021	Addressing Review comments	MOHAP
2.0	26-May-2021	Reviewed and Approved changes and baselined Version	MOHAP

Table 1: Version History

Document Acceptance and Sign-Off		
Name	**Signature**	**Date**
MOHAP		27-May-2021

Table 2: Document Acceptance and Sign-off

1 About this document

1.1 Purpose of this Document

The purpose of this document is to describe the solution being proposed to achieve SSO integration with the Riayati HIE. It will elaborate on the SSO interactions involved in the process, and the specific attributes that will be required in the Security Assertion Markup Language (SAML) token, and how they will be validated and processed.

1.2 Audience

This document is intended for the Participants (implementers) from the Health Organizations that are associated with Ministry of Health and Preventions (MOHAP).

1.3 Use Cases

Users of an Electronic Medical Record (EMR) system or other hospital system can launch the Riayati HIE Clinical Viewer for a specific patient in context, this is referred to as SSO access in “embedded mode”.

1.4 Abbreviations and Terms

Abbreviation	Term
EMR	Electronic Medical Record
ESB	Enterprise Service Bus
HIE	Health Information Exchange
HIS	Hospital Information System
IDP	Identity Provider
MOHAP	Ministry of Health and Prevention
SAML	Security Assertion Markup Language
SP	Service Provider
SSO	Single Sign-On
BTG	Break the Glass
UAE	United Arab Emirates
CV	Clinical Viewer

Table 3: Abbreviations and Terms

2 Introduction

2.1 Riayati Program

His Highness Sheikh Mohammed bin Rashid Al Maktoum announced in 2015 the initiative to establish a Health Information Exchange system – "RIAYATI" for patients in the Northern Emirates, UAE. In order to facilitate the movement of patients across healthcare providers, as well as connect public and private hospitals and clinics to share and exchange Health Records.

The Riayati Service will be the primary force driving an integrated, sustainable modern healthcare system that improves the safety of the patients, healthcare quality and population health in general through the safe sharing of medical data and information of all healthcare system beneficiaries across the Northern Emirates.

2.2 Health Information Exchange

Implementation of Health Information Exchange (HIE) within the Riayati services will enhance continuity of care among providers and create a sustainable and efficient health system. The care providers will have greater access to the patient's Health Data from across the healthcare entities. This will also result in reduction in errors in diagnosis and treatment and consequent reduction in hospital admissions and greater elimination of duplicate efforts such as duplicate laboratory tests. It will increase workforce productivity by reducing effort in repetitive activities when patient goes from one entity to the other.

This will result in reduction in readmissions resulting in cost savings to the UAE, better control on acute care episodes leading to reduction in hospital visits, improvement in quality of care and savings in prescription costs.

The Riayati Health Information Exchange will make quality healthcare data available for improvement of the patient care and support the futuristic innovative services like Clinical Decision Support, UAE specific clinical pathways, advanced analytics, and Artificial Intelligence.

The Riayati HIE has various components as mentioned below to support the objectives.

- **Unified Care Record (Includes the Core, ECR's and Registries):** a complete health information exchange solution for healthcare enterprises and information networks. Including Edge Gateway Cache Repository receiving live data from data sources with registries maintaining essential reference information
- **Bus, Access Gateway, and Clinical Viewer:** A gateway service that delivers aggregated data on patient records across ECRs and IHE ESB connections with a web-based viewer to access and display clinical records.
- **Operational Data Store (ODS):** An enhanced aggregated patient record cache hosting the FHIR Gateway for inbound FHIR queries
- **Patient Index (HSPI and linkage):** an enterprise master patient index solution that provides patient identity matching.
- **Web Gateway:** provides the communications layer between the hosting web server and Riayati HIE.

3 SSO Integration

The following SSO interactions are directly derived from the SAML 2.0 standard (see https://docs.oasisopen.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0-cd-02.html).

In SAML terms, Riayati HIE acts as "**Service Provider**" (SP). The role of **Identity Provider** (IdP) responsible for authentication should be assumed by the **EMR** embedding Riayati HIE's clinical viewer, a **third party IdP** acting on behalf of the EMR, or some **independent IdP** in the case of a stand-alone (non-embedded) access to the Clinical Viewer.

3.1 Identity Provider-initiated Single Sign-On (SAML 1.1)

This diagram illustrates the SAML 1.1. This approach relies on a peer-to-peer trust between the service provider and the identity provider. Every SP that can process a valid assertion from any other SP automatically trusts its server certificate.

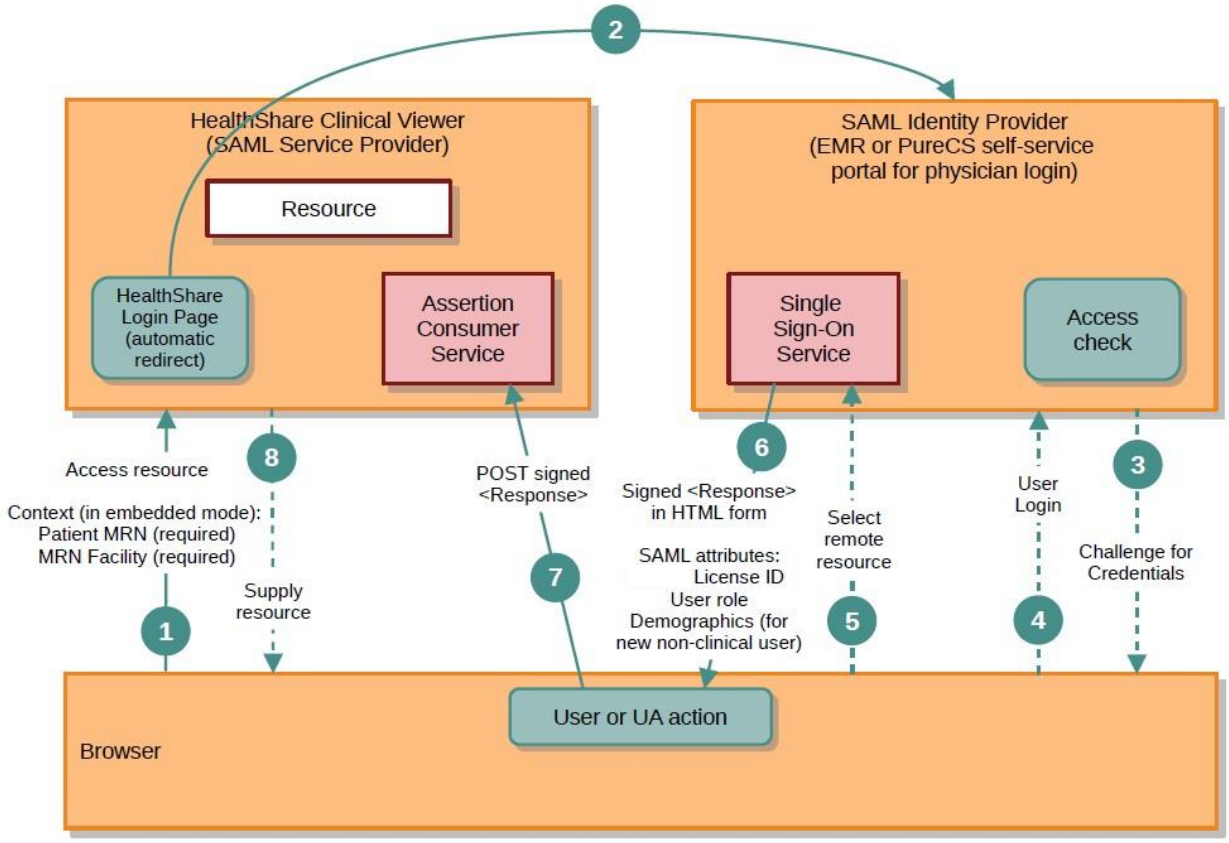

Figure 1: IDP initiated SSO

1) In an IdP-initiated SSO, **the user initially connects to the Identity Provider** that will prompt the user for credentials if a local security context does not exist. As illustrated in this diagram, the user experience can be somewhat improved by

   installing a special Riayati HIE login page that is triggered when a local security context is not available (the original URL does not contain a valid SAML assertion) and redirects the user to the relevant link on the IdP. **Note that in this case, selecting different IdPs depending on context requires an ad hoc, more complex implementation process.**

2) If the user does not have a valid local security context at the IdP, the user is challenged to provide credentials to the IdP site (otherwise skip to (5))
3) The user provides valid credentials, and a local logon security context is created for the user at the IdP.
4) The user selects a menu option or link on the IdP to request access to an SP web site. The IdP's SSO service gets called.
5) The SSO service builds a SAML assertion representing the user's logon security context. It **must include the Riayati required metadata** (see 5 SAML Attributes).
6) The assertion is digitally signed and packaged in a <Response> message. It is sent back to the browser that redirects it to the SP's Assertion Consumer Service.
7) Riayati HIE's Clinical Viewer will:
    a) validate the SAML assertion
    b) create a clinical user in the Riayati HIE User Registry, if required
    c) if a patient context is present, check if the patient exists and apply consent
    d) If patient has consent restrictions, then user must break the glass depending on their access policy.
    e) forward the request to the appropriate page in the Clinical Viewer

4 Solution Design

4.1 Prerequisites

SAML metadata for each Identity Provider must be available to Riayati HIE (as a service provider) for configuration.

The Identity Provider will provide X.509 credentials in SAML responses; **the public key of the CA that issued the credential for the IdP will be provided for Riayati HIE** configuration.

4.2 Accessing Clinical Viewer in embedded mode

This is the scenario where users of an Electronic Medical Record (EMR) system or other hospital system can launch the HIE Clinical Viewer for a specific patient in context.

It is possible that different systems use different Identity Providers. This can be supported by defining different SAML Service Providers in the HIE - each associated with a particular Identity Provider. These SAML Service Providers will provide unique endpoints which can be used by different EMRs depending on which IdP they use for SSO.

In addition to using the correct URL for the relevant SAML Service Provider, the 3rd party system must also provide the correct patient context in URL parameters. If the patient context is not present in the URL, the request will be rejected. This is described in detail in the following sections.

4.2.1 Patient Context

It is important to note that, when accessed in embedded mode, the user will be presented with the details of the patient identified by the patient context as received in the URL parameters. The user will not be allowed to navigate away from the patient's record to another patient e.g., by going to the Clinical Viewer's search page and searching for another patient.

This is to ensure that the record being viewed in the Clinical Viewer is always that of the patient that is being viewed in the application that embeds the Clinical Viewer (typically an EMR). This requirement is very important from a clinical point of view, to avoid confusion for the clinical user that may cause medical errors.

Similarly, the 3rd party applications embedding the Clinical Viewer must also ensure that the user cannot change the patient context in that system without closing the Clinical Viewer first, or that they will update the view on the embedded Clinical Viewer by submitting the right patient context. **The 3rd party application providers must be clearly informed of this requirement, since the Clinical viewer has no way to detect that kind of context change on its own**.

4.2.2 Patient consent

In the embedded mode, once the SAML assertion has been validated, the HIE will search the Patient Registry using the patient context received in the URL. The patient consent will be automatically applied at this step, based on patient's MPI Consent Policy as defined in the Registry.

If the patient does not exist, the request will be rejected. If patient has consent restrictions user will be required to break the glass based on access policy. If user access policy does not allow break the glass, then clinical data will not be visible in Clinical Viewer.

5 SAML Attributes

5.1 Functional description

The Riayati HIE will support the following SAML attributes in the request.

5.1.1 User Id

One of the following attribute(s) must be present for user identification.

1. User License Id – Required for a clinical role. If present, only this attribute will be used to check if the user exists in the HIE Clinician's Registry. If a user is not found in the HIE Registry, the HIE will attempt to fetch the user details using the "Find a Doctor" service. If the service successfully returns user details, the user will be created in the HIE Registry using the HIE - "Find a Doctor" integration. Otherwise, the request will be rejected.

When a user logs into the Clinical Viewer using SSO for the first time, a new login id for the user will be created in the appropriate Security Domain. The user role received in the SAML assertion will be associated with this login id.

5.1.2 User Role

The user role must be present in the SAML assertion. It must be one of the standard Riayati HIE user roles e.g. %HS_Clinician, %HS_Nurse, etc.

Following is the list of user roles with the access supported in Riayati HIE:

Riayati HIE Role	Definition	Access
%HS_Clinician	All registered clinicians primary care, specialist etc.	A "Clinician" will be able to search patients and view all medical record information available in HIE. A Clinician **will not be able** to access sensitive data by breaking the glass feature.
%HS_Clinician_BTG	All registered clinicians primary care, specialist etc.	A "Clinician_BTG" will be able to search patients and view all medical record information available in HIE. A Clinician_BTG will be able to access sensitive data by breaking the glass feature.
%HS_Nurse	All types of nurses, residents, physician assistants who provide healthcare services under supervision from physician	A "Nurse" will be able to search patients and view all medical record information available in HIE. A "Nurse" **will not be able** to access sensitive data by breaking the glass feature.
%HS_Nurse_BTG	All types of nurses, residents, physician	A "Nurse_BTG" will be able to search patients and view all medical record

	assistants who provide healthcare services under supervision from physician	information available in HIE. A "Nurse_BTG" can access sensitive data by breaking the glass feature.
%HS_AlliedHealth	All users who provide healthcare services such as Pharmacist, Therapist, Psychologist, Medical Technologist, Dietitian, Medical Student but are not considered as physician/ nurse	An Allied health professional will be able to search patients and view Demographic, Allergies, Medications, Encounters, Problems & Diagnosis, and Results information only. An allied health professional will not be able to access sensitive clinical data.

Table 4: Riayati HIE Role Matrix

Note: Non-clinical users i.e., Clerical users access will not be supported in Riayati HIE.

If the role is blank or invalid, the request will be rejected.

If a clinical user already exists in Riayati HIE Registry and a login id in the appropriate Security Domain also exists, the existing roles associated with the login id will be removed and replaced with the user role in the current SAML assertion. This will allow the same clinical user to log into Clinical Viewer with different roles at different times.

5.2 SAML attributes

The following attributes will be used:

Attribute	Required	Type	Notes
clinicianId	Yes	String	Must be a valid clinician license id. Identifies a clinical user.
urn:oasis:names:tc:xacml:2.0:subject:role	Yes	String	Must contain a Riayati HIE-formatted role

Table 5: SAML Attributes

6 URL Parameters

6.1 Functional description

The following details can be required to be passed as URL parameters when the Clinical Viewer is accessed using SSO.

6.1.1 Patient Context

In embedded mode, the patient context must be present so that the user can be presented with the correct patient's record. Otherwise, the request will be rejected.

1. Patient MRN
2. Facility License Id (*License ID of the facility initiating the SAML request, it should be same as configured for sending facility(MSH.4) in HL7 messages or CCDA.)*

6.2 Proposed parameters

The following URL parameters are suggested. They will be finalized in the Solution Design Document.

The values must be URL-encoded as relevant.

URL parameter	Notes
mrn	Required in an embedded scenario.
facility	Required in an embedded scenario.

Table 6: Proposed URL parameters

7 Record Indicator API

7.1 Objective

The objective of this REST API is to identify whether the Riayati Unified Care Record has any patient records from the other Facilities / Organizations. This API will resolve the Patient based on Patient's MRN and Facility and will exclude the Patient records from same facility and the Organization (OMRN Assigning Authority) based on parameter.

7.2 Pre-requisite for Implementation

The below activities should be performed as a pre-requisite for the Riayati Record Indicator Integration.

- The EMR/HIS system should have the capability to perform a GET from the REST endpoint using the arguments listed.
- Record indicator flag should be embedded within EMR/HIS system.

7.3 Implementation

- Riayati HIE will allow to perform the GET operation by calling the REST API endpoint.
- Below is the list of arguments to specify in GET REST API call and the response values.

Arguments	Notes	Required
mrn	Patient MRN in the EMR application	R
facility	Facility ID of the MRN	R
omrn-authority	Assigning Authority of the Organisation level MRN.	O

Table 7: Riayati HIE – Record Indicator Argument List

- The Organization level MRN can be used only when the EMR/HIS system supports multitenancy (multiple facilities are hosted with single EMR/HIS instance) and there is a common/centralized/community MRN identifier for all the facilities.

Response Values	Notes
flag	true or false. Indicating if Riayati holds data from some other facility or some other organisation.
num_sources	Number of data sources other than the requestor that contributed to the patient's unified care record.

Table 8: Riayati HIE – Record Indicator Response List

- A value of true for "flag" means that Riayati holds data from another facility or another organisation for the Master Patient Index (MPIID) in Riayati Patient Registry associated with the local MRN provided.
- A value of false for "flag" means that at least one of the three conditions below is true:
    - Riayati is not aware of this MRN.
    - All the clinical data in Riayati comes from the same requestor (querying facility or organisation) that is associated with the record indicator client.

- The value in "num_sources" indicates the number of data sources other than the requestor's that contributed to the patient's unified care record.

7.4 Record Indicator REST Endpoint

The URL to access the Record Indicator from the EMR/HIS system will be:

GET https://<baseURL>/csp/healthshare/hsregistry/riayati-api/recordindicator?mrn=<Local-MRN>&facility=<FacilityID>