WISCONSIN
INTERACTIVE
NETWORK

Wisconsin Enhanced Prescription Drug Monitoring Program (ePDMP) Integration Service

Technical Specifications

Table of Contents

Service Overview

The service integration between the State of Wisconsin Enhanced Prescription Drug Monitoring (WI ePDMP) system and an organization's electronic health records (EHR) system exists for the following purposes:

- Securely identify the EHR system and the EHR user as an authorized WI ePDMP user and authenticate them.
- Allow the EHR user to view a patient's WI ePDMP Prescription History Report from the EHR system without having to re-enter query parameters such as first name, last name and date of birth.
- View the Patient History Report as HTML inside browser in the EHR (work to be completed by each EHR system).
- Capture an audit trail about the query and the user who performed it. (Note: available only in the WI ePDMP website directly.)

Out of state queries are excluded from EHR Integration. If you need to query states other than Wisconsin you will need to use the full ePDMP Website.

EHR System Owner Responsibilities

Each EHR system owner will be responsible for any and all costs associated with work required to complete the work necessary to integrate with the WI ePDMP. This includes:

- Assignment of the appropriate project resources, which may include:
  - Project Manager: Functions as a single point of contract for WIN team. Manages and coordinates all EHR system resources.
  - Development Resources: Completes necessary work on the EHR system to connect to the ePDMP.
  - Executive sponsor: Provides all final approvals and sign-offs for the implementation.
- Adhering to the timeline, as jointly established.
- Development of test cases and coordination of all testing resources.
- Provide a test/UAT environment.
- Provide the URL value for the OAuth Authorization URL
- Provide the URL value for the OAuth Token Exchange URL.
- Provide the URL value for the OAuth ISS URL
- Client machines that access the WI ePDMP must accept cookies in web browsers
- Client machines that access the WI ePDMP must be able to run javascript in web browsers
- Note: The system owner is responsible for notifying WIN at least 7 days in advance of changes to the Authorization, Token Exchange, and/or ISS URL. Failure to notify WIN of changes will result in your integration to become unusable.

Technical Overview

- Use SMART on FHIR with OAuth standards to allow a user of the EHR system to be identified and authenticated as an authorized WI ePDMP user by the WI ePDMP system from within an existing EHR user session.
- Link to search the WI ePDMP from within the EHR system.
- Connect via TLS.
- Initial launch request will include EHR System ID, launch token, timestamp, and SMART on FHIR server information to authenticate the request.

An example request might look like this:
https://pdmpuat.wi.gov/ehr-query/query-launch?hcsid=<PARAMETER>&iss=<PARAMETER>&launch=<PARAMETER>

- The reply to the query-launch request will be a browser redirect to the SMART on FHIR authorize endpoint. The SMART on FHIR authorize endpoint will redirect back to the WI ePDMP system with access code and session state parameters.

An example request might look like this:
https://pdmpuat.wi.gov/ehr-query/patient-report?code=<PARAMETER>&state=<PARAMETER>

- The WI ePDMP will execute an HTTP POST and send the code value received back to the SMART on FHIR Token Exchange endpoint. The reply to the POST request will be the access token payload.
- The access token payload will include the EHR system User ID of the user performing the query, which will be used to confirm they have an active account with the WI ePDMP. Additionally, the access token payload will include required launch parameters for patient first name, patient last name, patient date of birth and optionally, a facility ID.
- ePDMP will use the launch parameters to associate the EHR system user with a user account in the ePDMP.
- ePDMP will use the launch parameters to execute a patient query and return HTML.
- Use browser in the EHR system to display the HTML Patient History Report.
- Links the User ID in the EHR system to the user's WI ePDMP account.

Technical Implementation

- Every EHR system has their own OAUTH server. Every EHR system will provide WIN with their OAUTH URLs for launch/code/token exchanges and the "base url" at the time of setup. WIN will not use the URL information passed along on the initial launch request. WIN creates an application definition within their OAUTH server. WIN provides the urls to redirect back. WIN stores the OAUTH client ID (GUID).
- Establish a public end point for the EHR system

- Accept SSO token and EHR System ID
- Validate EHR System ID
- Check SSO endpoint to validate token
- Link list of EHR system-provided User IDs with the ePDMP account

Field Information

Data to be included in the querystring for EHR system identification:
The EHR System ID (defined and provided by WIN) (hcsid)
The Launch Parameter as supplied by the OAuth SSO (launch)
The ISS URL value of the the OAuth SSO Server (iss)

Launch parameters to be included in the access token payload for user identification:
The Facility ID (optional)
EHR system User ID

Launch parameters to be included in the access token payload for patient search:
Patient’s first name
Patient’s last name
Patient’s DOB (mm-dd-yyyy)
Patient’s Zip Code (optional)

Example access token payload:

```
{
  "access_token":"xj5JbZHd<TRUNCATED>NqV9bAUOcP6OzEE",
  "token_type": "bearer",
  "expires_in": 3600,
  "FACILITY_ID": "10501101",
  "PATIENT_DOB": "1954-01-06",
  "PATIENT_FIRST": "Sherlock",
  "PATIENT_LAST": "Holmes",
  "PATIENT_ZIP": "53528",
  "USERID": "WISCOMD",
  "need_patient_banner": "true",
  "patient":"TeL-9BK2<TRUNCATED>JDfoB",
  "smart_style_url": "https://<BaseFHIRUrl>/FHIR-2016-
Secure/api/2016/EDI/HTTP/style/100010/I0YyRkFG<TRUNCATED>lcmlmfHw%3D.json"
}
```

Data for account initialization:
The CSV File for pre-associating EHR users with PDMP users should have four fields. The file should not have a header row.

- EHR system User Id - This is the user id value used by the EHR system
- DEA Number - This is the DEA Number of the user
- License Number - This is the license number of the user
- Reg Code - This is the code detailing the type of license (e.g. 15 - Dentist)

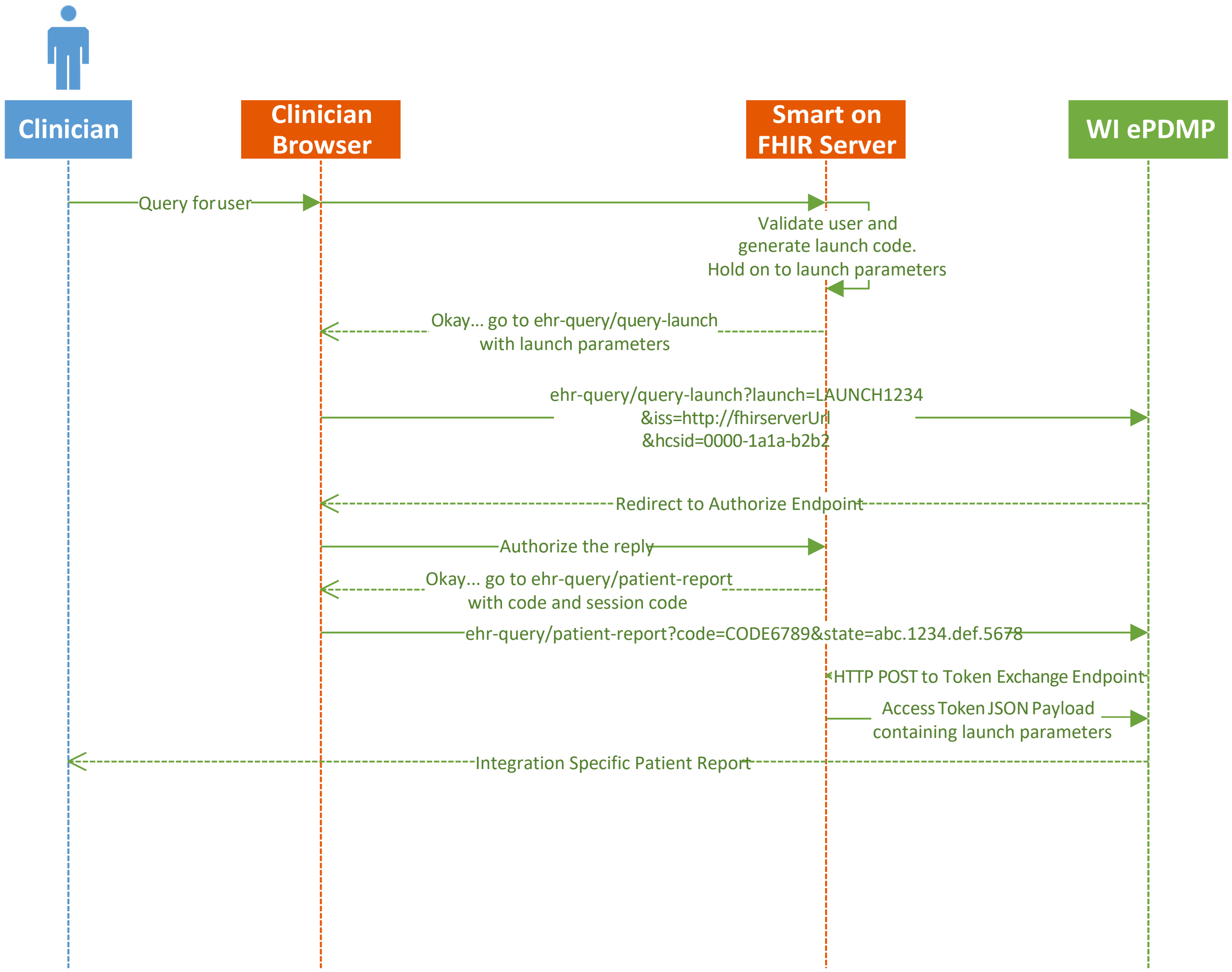
```
ARGONAUT,BC5988312,1687,15
ARGONAUT2,,1290,15
ARGONAUT3,BY7305813,,
ARGONAUT4,XX1234567,1234,99
ARGONAUT5,XX1234567,,
ARGONAUT6,,999999,99
ARGONAUT7,XX1234567,123A4,99
ARGONAUT8,XX1234567,1234,B99
```

A list of the above information will be provided by the EHR system to WIN as part of the implementation process. This will allow these accounts to be linked to each individual user's respective ePDMP accounts. If an ePDMP account has not been created, that account will be provided in a list for the EHR system.

Workflow

1. EHR system user signs into EHR.
2. EHR system user looks up patient record in EHR.
3. Health care system user clicks on a link in the EHR system to lookup up patient in WI ePDMP.
4. The WI ePDMP authenticates the request via OAuth2 mechanism.
5. The WI ePDMP system checks to determine if the EHR system User ID is already linked to their WI ePDMP account.
    a. If WI ePDMP user is not already linked with the EHR system User ID, then the user is redirected to a validation screen "We couldn't find you, please enter your username and password for the WI ePDMP.".
        i. The EHR system user enters their WI ePDMP username and password.
            1. If the WI ePDMP user's account is found, the EHR system User ID is linked to the user's WI ePDMP account.
            2. If the WI ePDMP account is not found, the user is allowed to re-enter the WI ePDMP username and password.
        ii. The user is allowed to navigate to the WI ePDMP registration screen.
    b. If EHR system User ID is already linked with a user in the WI ePDMP, the patient query is executed.
        i. If a patient exists in the WI ePDMP, the Patient History Report is displayed via HTML in a browser window.
        ii. If the patient doesn't exist in the WI ePDMP, a message is displayed via HTML in a browser window.
6. The returned window will time out after the normal WI ePDMP session timeout.
7. Possible errors that will be handled with messaging:
    a. Failed SSO.
    b. EHR system not active or not registered.
    c. Attempted patient search with an invalid account type.
    d. WI ePDMP user account is invalid, inactive, password/username is incorrect.

Logical Sequence Diagram


Clinician
Clinician Browser
Smart on FHIR Server
WI ePDMP
Query foruser
Validate user and generate launch code. Hold on to launch parameters
Okay... go to ehr-query/query-launch with launch parameters
ehr-query/query-launch?launch=LAUNCH1234 &iss=http://fhirserverUrl &hcsid=0000-1a1a-b2b2
Redirect to Authorize Endpoint
Authorize the reply
Okay... go to ehr-query/patient-report with code and session code
ehr-query/patient-report?code=CODE6789&state=abc.1234.def.5678
HTTP POST to Token Exchange Endpoint
Access Token JSON Payload containing launch parameters
Integration Specific Patient Report

Frequently Asked Questions

- What is the size of the window that is displaying the Patient History Report?
  - This is dictated by the healthsystem
- Are the time out parameters in this integration the same as in the ePDMP application?
  - Yes, the timeout is 15 minutes.
- What healthsystem ID is this integration using?
  - When the healthcare system is initially setup, WIN will provide an id value that will need to be used when making requests.
- Does this integration support storing the healthsystem ID or is the health system storing it?
  - Both the healthsystem WIN will be storing the ID.
- Does this integration support delegates?
  - Yes, this integration supports delegates. Delegates cannot be pre-linked and the initial login through the EHR patient search process will link the EHR account to the PDMP account.
- Does this integration support multiple patient results?
  - Yes, the multiple patient's will display on the Patient History Report selection screen as they do on the web application.
- What changes do the health systems need to make for this integration?
  - Please review the Smart on FHIR requirements and work with your health system vendor on their configuration requirements.
    - https://smarthealthit.org/
    - http://docs.smarthealthit.org/
    - http://docs.smarthealthit.org/authorization/