~~California~~ Department of Justice (DOJ)

Controlled Substance Utilization Review and Evaluation System (CURES) Information Exchange Web Service

Overview

~~July~~November 2021~~December 2019~~

The purpose of this document is to provide an overview of the CURES Information Exchange Web Service. Outlined below is a brief explanation of the technology, as well as the use cases, associated with this web service.

The CURES Program will provide systems integration with the Health Information Technology (HIT) community through RESTful web services. For the initial phase, the following web services will be available to serve the following functions:

- Searches for a patient for a given timeframe
- Retrieves a patient controlled substance history
- CURES and a HIT system's user account status

Information will be exchanged using NCPDP SCRIPT XML REST-based format. Searches can be executed for a period using partial or exact match modes.

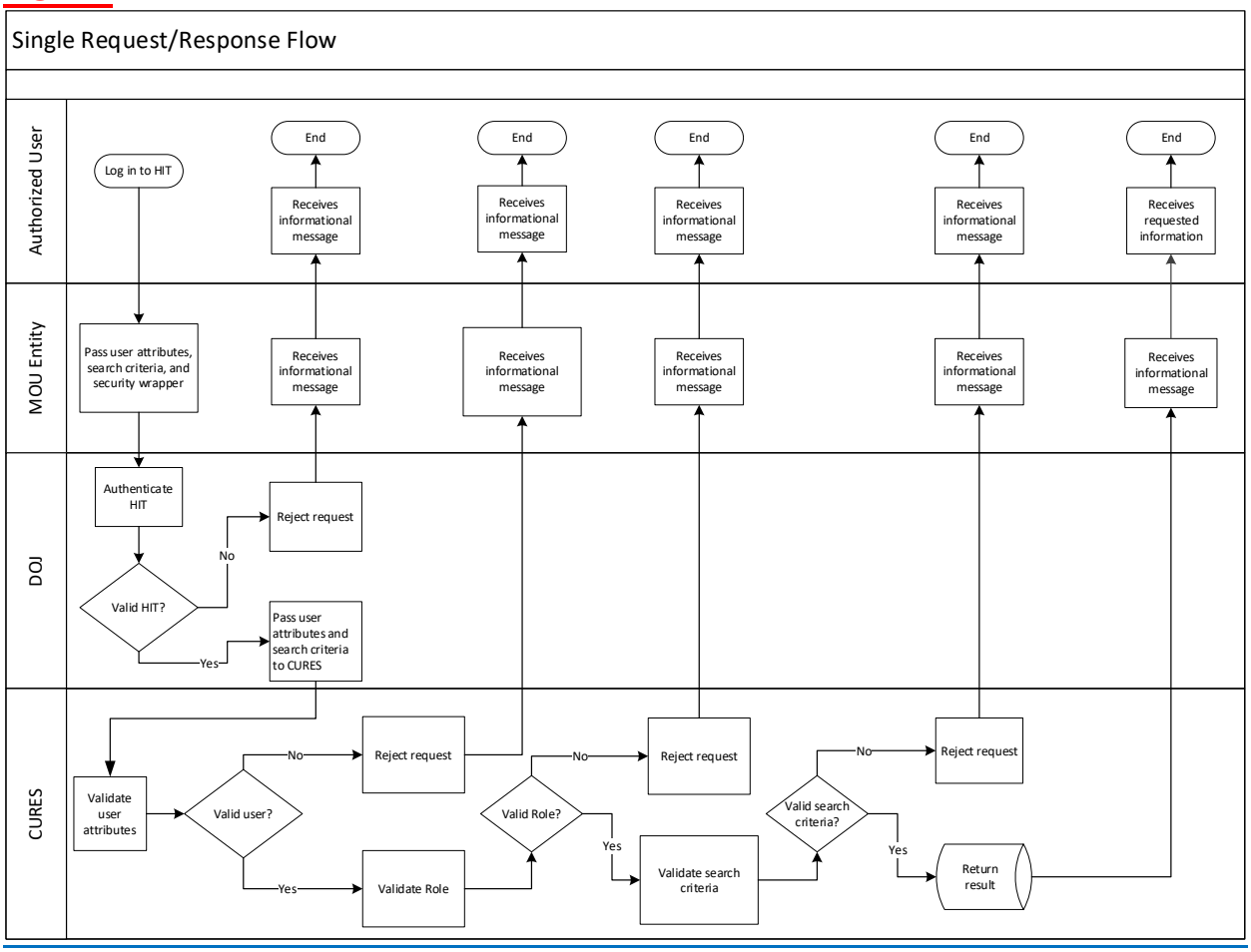
Search Patient and Generate Report

The CURES web service will support two patient search use cases:

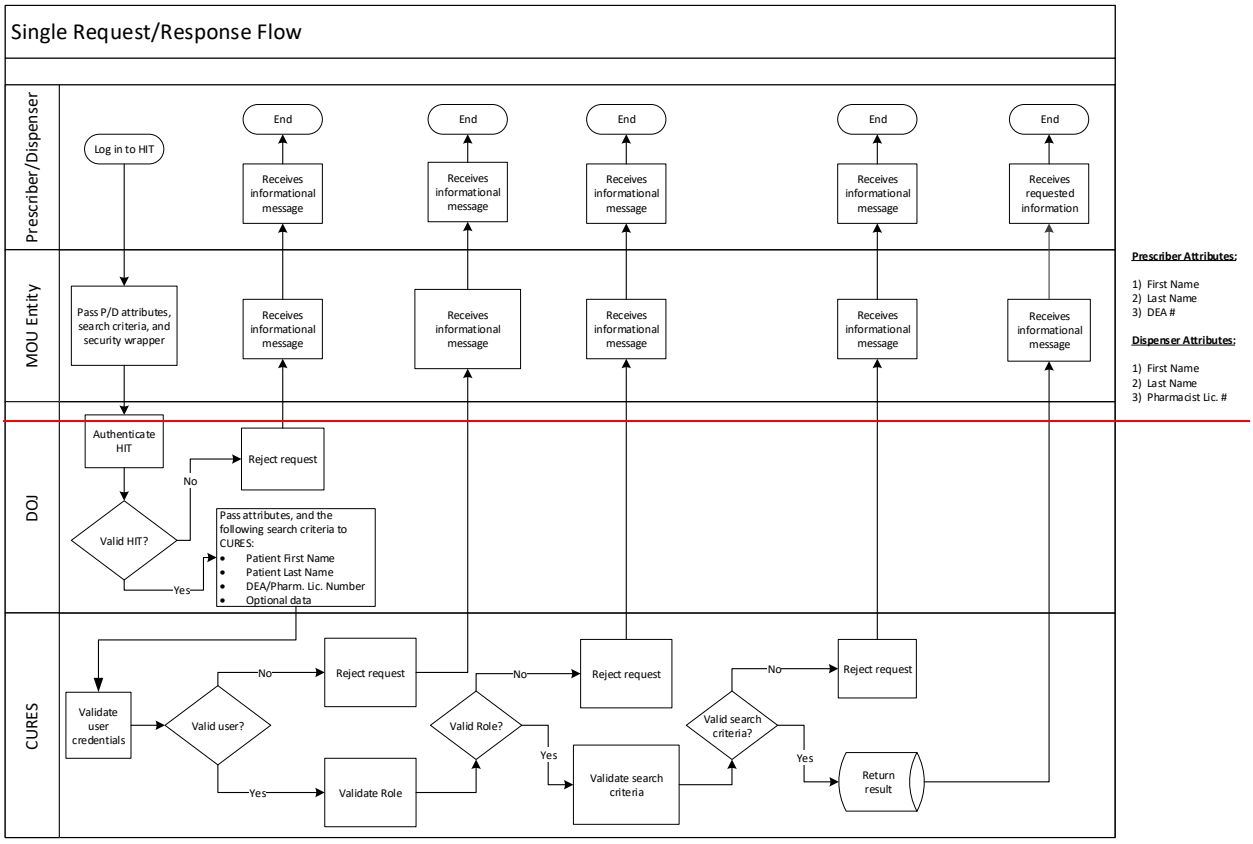
- Query Use Case 1 – Single Request/Response
  - Use Case 1 follows the NCPDP standard where every search patient request returns either no match or a single match. The result will be either an error message stating there is no match, or will return all of the prescription history associated to the matched entity.

Figure 1 – Single Request/Response

ADD NEW FIGURE 1 BELOW TO REVISED FORM



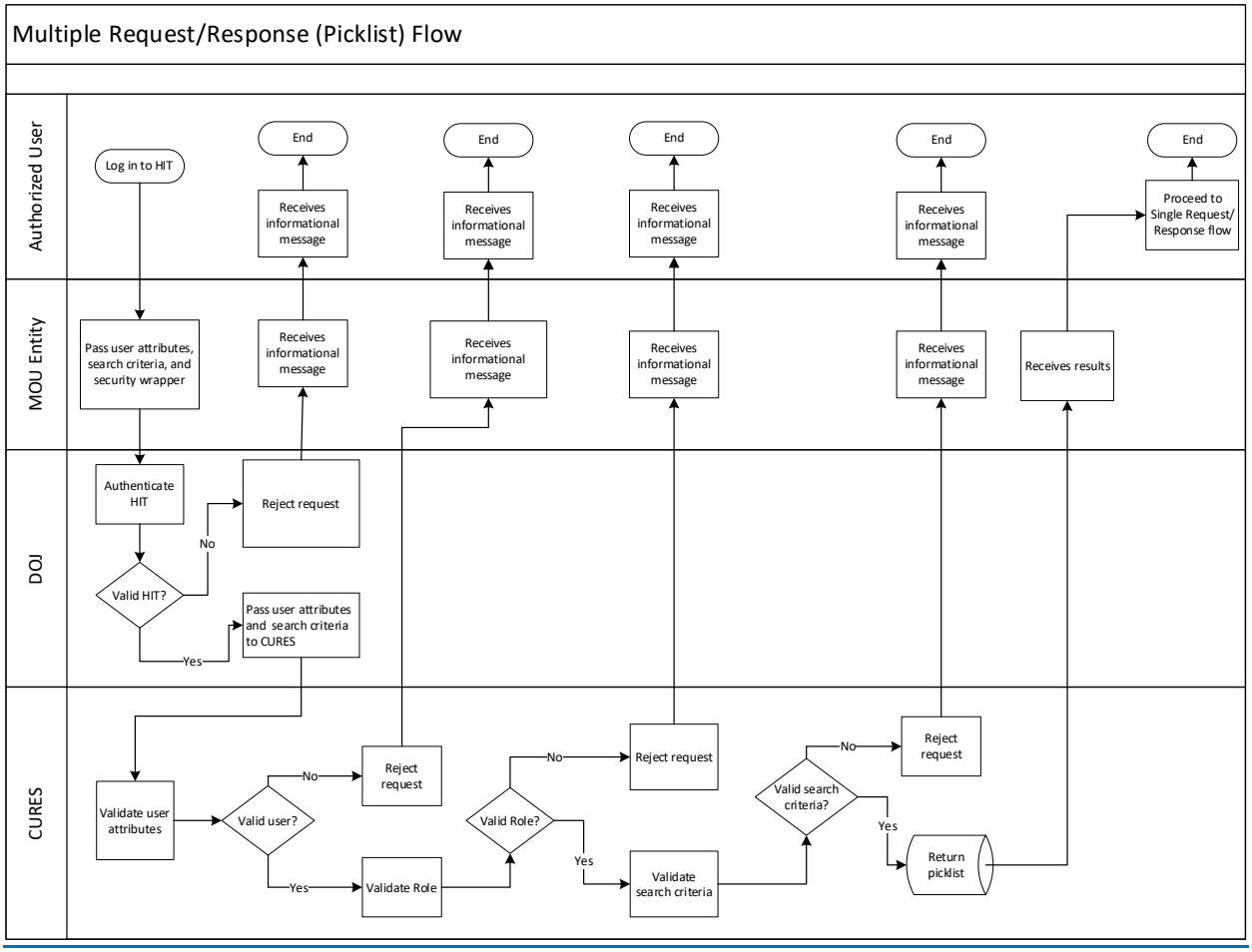
DELETE EXISTING FIGURE 1 BELOW FROM REVISED FORM



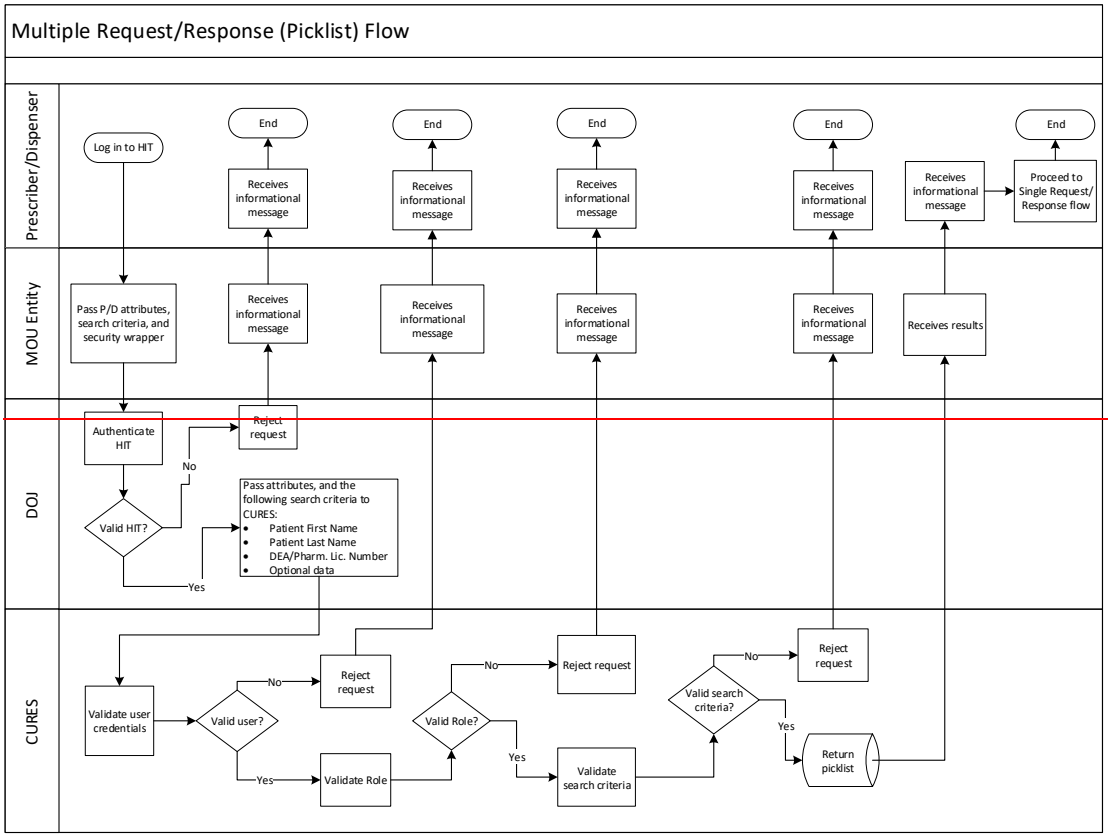
- Query Use Case 2 – Multiple Matches (Picklist)
    - Use Case 2 supports multiple matches, via a picklist~~pick list~~. In this use case, a patient search returns multiple entities using a NCPDP-like message structure. The requesting entity would then send one or multiple single requests to retrieve the prescription history associated to the matched entity.
    - For those HIT systems that cannot support this functionality, a response message redirecting the health care practitioner/pharmacist to the CURES web application is returned.

Figure 2 – Multiple Request/Response

ADD NEW FIGURE 2 TO REVISED FORM



DELETE EXISTING FIGURE 2 BELOW FROM REVISED FORM



Account Status Check

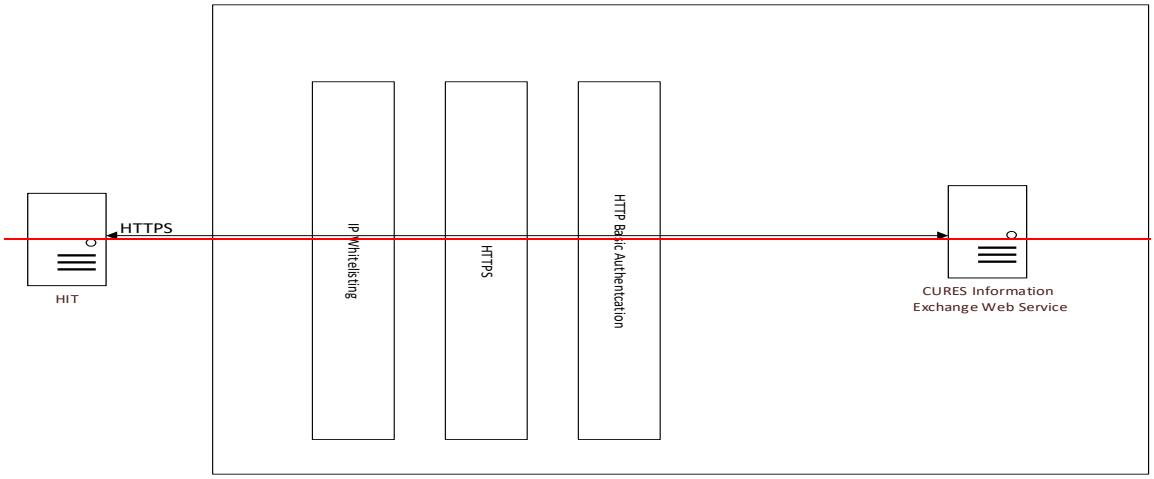
In addition to the query use cases, the CURES web services will provide web services to query for account status. The first allows the HIT systems to query for the CURES user account status. The second allows the HIT systems to query for their own account status. These services allow the HIT systems to troubleshoot and alter process flows based on account status.

Security

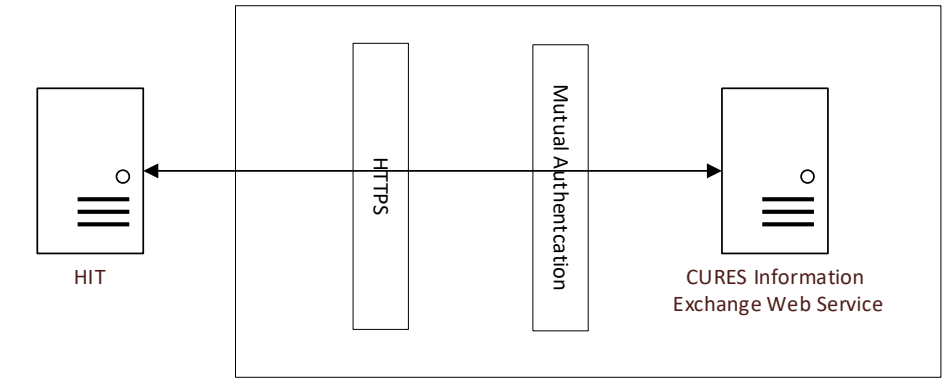
The CURES web service has ~~three~~two layers of security. Each layer is built on top of the previous to ensure the secure exchange of information. Each REST endpoint is stateless, resulting in every request going through all ~~three~~two layers.

Figure 43 – Security Layers

DELETE EXISTING FIGURE 4 BELOW FROM REVISED FORM



ADD NEW FIGURE 3 BELOW TO REVISED FORM



~~**Network Security**~~

~~IP whitelisting will ensure only enrolled HIT systems can communicate with the CURES web service.~~

Network Communication Security

Communication between the CURES web service and the HIT systems will be over the Internet. As a result, Transport Layer Security (TLS) is required to ensure secure communication between CURES web services and HIT.

Access Security

After entering into a **Memorandum of Understanding (**MOU**)** with the Department of Justice, HIT systems will be authenticated by their client certificates. HIT systems will also verify that they are talking to the right server by verifying the server certificate.~~provisioned with a CURES web service account.~~ Every RESTful web services request should be accompanied with the credentials and will be validated to ensure the account is valid and in good standing.

Mutual Authentication

An entity that has entered into an MOU with the Department of Justice will need to have a private and public certificate pair. The entity will keep its private certificate and send the public one to the Department of Justice. This certificate pair will be used for encrypting and decrypting messages and authentication purposes.