IIR
Institute for Intergovernmental Research

PDMP TTAC
Prescription Drug Monitoring Program Training and Technical Assistance Center

RxCheck

Prescription Drug Monitoring Program

RxCheck Integration Guidance Document

November 2020

This project was supported by Grant No. 2019-PM-BX-K003 awarded by the Bureau of Justice Assistance (BJA). BJA is a component of the U.S. Department of Justice's Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking (SMART). Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice.

In 2002, Congress appropriated funds for implementation and enhancement of prescription drug monitoring programs (PDMPs) through the Harold Rogers PDMP Grant Program. From its inception, the grant program has been administered by the Bureau of Justice Assistance (BJA), Office of Justice Programs, U.S. Department of Justice (DOJ). The grant funding supported states in implementing PDMPs, with an increase in the number of PDMPs from 16 (2002) to 54 (2020). The dramatic increase in PDMPs led to the realization that there was a need for interstate data sharing. BJA appropriated funds that allowed PDMPs to develop and implement an interstate data sharing solution. In 2005, the BJA/IJIS PDMP Committee was formed. It was composed of state, federal, and IJIS representatives with the goal to implement a standardized approach for the exchange of data among states and establish a PMIX Hub as the focal point for execution design. A successful test of information exchange was completed with California and Nevada in 2007, and a national open standards-based PMIX capability, which conforms to the National Information Exchange Model (NIEM), was adopted. By 2010, the PMIX Hub installation was completed and active for transactions between Ohio and Kentucky. The next year, the PMIX Hub became the RxCheck Hub, and RxCheck Governance Board was established. Initially, the membership of the RxCheck Governance Board consisted of 11 PDMPs with 3 PDMPs connected, but the membership has since grown to 24 members with 32 PDMPs connected in June 2020. An additional 17 PDMPs are in the process of being connected to the RxCheck Hub. In 2018, BJA/CDC began a pilot project to integrate PDMP data with electronic health records (EHRs) through the RxCheck Hub; three PDMPs successfully integrated with EHRs (Illinois, Kentucky, and Utah).

The following provides an overview of the integration process for the RxCheck Hub.

I. Types of Connections

Data exchange allows data to be shared between different systems through a source schema and transforming it into the data structure of a target schema. The RxCheck Hub offers flexibility in the types of data exchange types allowed for integration:

- NCPDP v10.6
- NCPDP 2017
- HL7 FHIR 3.0 and 4.0
- PMIX XML

In addition, the RxCheck Hub provides several integration connection options:

- SRS client installation – SOAP
  - Single-site version
  - Enterprise version
- FHIR API Installation
- Connections initiated by state PDMP and partner organizations (PDMP contacts)
  - State-managed, role-based permissions
  - Local health care system or vendor administration of hub configuration

For assistance with any technical issues, support is available upon request. A request can be sent by completing an online form or by reserving a time slot.

II. Detailed Description of RxCheck Integration Features

The RxCheck integration features described below are designed to ease the level of effort needed for integration.

Health Entity Onboarding Requests

Health care entities (HCEs) and health information exchanges (HIEs) wishing to take advantage of the free RxCheck integration solution (no connection, user, integration, licensing, transaction, or recurring fees) should complete the Integration Request Form as the first step to integrate their HCE/HIEs with their states' prescription drug monitoring programs (PDMPs) via RxCheck. The integration request form is available upon request.

Once completed, the integration request will be automatically routed to the PDMP administrator's inbox for consideration of your integration connection request. The state PDMP administrator may request additional information before a decision is made. The administrator can then review and authorize the request in the public-facing page outside the console. If the request is approved, the administrator can configure the entity for operation, which creates the connection for the entity. The details of the request form are automatically copied over to the HCE page. Any questions related to your request to integrate or for needed assistance should be directed to the state PDMP (PDMP contacts).

III. Partnership With State PDMPs

The initiation of integration starts at the state level and is driven primarily by states. The RxCheck Hub provides support to HCEs on behalf of the state, as needed, to meet the state's objectives.

IV. Overview of RxCheck Security

RxCheck uses the national PMIX Architecture to enable interstate sharing of PMP data. The use of open, consensus standards promotes interoperability. The PMIX architecture requires (1) compliance with Global Reference Architecture (GRA) Reliable Secure Web Services Profile; (2) common National Information Exchange Model (NIEM) exchange data and metadata; (3) hub connections (and hub-to-hub capability); and (4) end-to-end security (including encryption key management).

The architecture has a shared infrastructure to support certificate/key management capabilities and basic directory services, specifically the PMIX Directory Service. The PMIX Directory, also known as the PMIX LDAP Server, provides for X.509 certificate management and public key exchange as well as PMP contact and service requirement information.

Core Principles: The following core principles are utilized to guide the development of other PMIX artifacts:

- **Distributed data sources**: Assumes distributed, rather than centralized, information sources.
- **Maintenance of state-level controls**: PMIX implementation will not impact or modify a state's control over the operation of the PMP and authorization to access prescription data.
- **End-to-end security**: Mechanisms must be utilized to ensure the security of PMIX in-transit data between the sending and receiving end points.
- **Information traceability**: PMIX data flows will leave an audit trail, not to include protected health information (PHI), to enable reporting on demand to PMP administrators.
- **Standards-based information sharing**: PMIX standards will leverage open industry standards such as Extensible Markup Language (XML) and the National Information Exchange Model (NIEM) for encoding data to ensure maximal interoperability between future exchange partners.

Security Classification

The patient health information exchanged by this service is assumed to be subject to strict privacy requirements (i.e., at least as strong as those required by the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA)) in every participating jurisdiction.

The hub routes messages using the WS-Addressing standard and forwards encrypted content without intervention using WS-Security.

Service Security

Message exchanges between states are protected using message-level security from state to state. Secure conversations can be established between states through the hubs with the request/response contents (message body) encrypted.

Independent transport security sessions using Secure HTTP are established between the requesting state and the hub and between the hub and the receiving state. Transport security is being used to ensure that the message headers are encrypted during transfers but visible to the hub(s) for routing and logging purposes.

PMIX message metadata is included in the unencrypted (but signed) message header to permit logging.

Service Privacy

PMIX requests and responses routed through a hub are securely transmitted using message-level security and federally approved data encryption standards. This encryption of the Protected Health Information (PHI) will effectively prevent the data from being visible to the PMIX Hub or from any other intermediate network node. The message-level encryption occurs between partner states, and, as a result, implementation of the encryption service is a responsibility of the partner states.

Other RxCheck Security includes the following:

- The RxCheck Hub is hosted on Azure Government Cloud, and the infrastructure is CJIS-, HIPPA-, and FedRAMP-certified.
- The Azure Government Cloud infrastructure is disaster-proof for business continuity by scaling the application in multiple regions in the country.
- All RxCheck servers are Linux servers, and Azure infrastructure is configured to detect any intrusions.
- OWASP coding standards are performed on RxCheck Hub source code.
- RxCheck is compliant with NIST 800-53.
- All connections undergo conformance testing and certification.
- Third-party penetration testing and SOC2 Type 2 audits are performed annually.

Options for connecting to PDMP:

RxCheck State Routing Service (SRS)

The SRS supports the following standards and, where needed, automatically translates the messages:

- NCPDP v10.6
- NCPDP 2017
- HL7 FHIR 3.0 and 4.0
- PMIX XML

RESTFul HTML Endpoint

The RESTful HTML endpoint is one of the interfaces provided by the RxCheck Hub to enable health care entities to securely connect and retrieve patient prescription information from the PDMP databases. The RESTful API supports a POST method for sending the request information in NCPCP 10.6 or NCPDP 2017 format to the RxCheck Hub. The interface is secured over HTTPS using username and password authentication for securely connecting to their SRS instances. The username and password can be securely configured using the RxCheck console. The integrating systems will receive a response to the query with the patient data, which includes the prescription history, pharmacy history, and patient demographics in an HTML format. The HTML format is complete with all necessary rendering tags that can be rendered on any standard browser frame. The integration entity will be able to directly integrate this output and display it directly within the EHR application. The HTML response will be formatted into a human-readable output for both valid successful responses and any error responses as well. The integrating entity, in conjunction with the PDMP, can customize this page to suit its needs. The RxCheck Hub does not see this detail; no PHI is visible, since the message is encrypted.

Management of Data Sharing Connections

Transaction Monitoring:

States can view and monitor real-time transactional data, as recorded in the Hub Audit Logs.

The RxCheck Hub Audit Log captures the following information:

Title	Description
Audit ID	Unique message identifier generated by the Hub
Request ID	Message identifier sent by the requesting health entity
Requesting Site	State PDMP, health entity, or facility sending the request
Disclosing Site	State PDMP disclosing the prescription report
Requestor	Name of the provider requesting the prescription report

Role	Provider role
DEA	DEA# of the provider
NPI	NPI# of the provider
Request Datetime	Date and time the request was made
Response Datetime	Date and time the response was sent back
Response Status	Status of the request (Provided/Deferred/Not Found etc.)

Configuration of Endpoints

Instructions and details pertaining to the configuration of endpoints can be found in the 'SRS installation and Setup Guide for PDMP' document.

Throttling

The throttling feature in the RxCheck Hub enables the PDMP administrator in each state to control the volume of messages coming into the PDMP system. Each state PDMP system is built with a request-handling capacity that is built within the system. If there are sudden increases in the flow of messages to the PDMP systems, then there could be potential performance implications for PDMP servers. To support a state in preventing the overloading of its state systems, RxCheck Hub provides a mechanism by which this overloading can be prevented. The "throttling" feature is a value that the PDMP administrator can control through the RxCheck console. The PDMP administrator can log in the state RxCheck console and configure the throttling value by setting the number of messages that the state system can handle over a period of time. This value can be configured based on the maximum allowed messages per second, minute, day, or month. The RxCheck Hub will track the number of transactions that are going through the hub and, when the maximum amount is reached for a set period of time, the Hub will reject all incoming messages to the PDMP system and prevent the overloading. Once the transaction limits fall below the maximum configured values, the RxCheck Hub will automatically start allowing transactions to flow to the PDMP systems.

V. Administrator Console

The administrator console displays the status of each integration: Name, Code, Status, Integration type, and the Date and Time the site was added.

Dashboard Menu Option	Dashboard Icon	Description
RxCheck Dashboard		Shows data from inbound and outbound transactions.
State Routing Service Configuration		Tells who hosts the entity's connection (entity IT or vendor), premise of cloud-based, persons who have access to the servers (all must be U.S.-based per SOC 2).
Hub Audit Logs		Captures real-time transaction details of request(s) and response(s).
Health Care Entities		Enables PDMP administrators to add/manage Health Care Entities, Site Details, Contact Details, Vendor Details, Manage Roles, and User Administration.
Interstate Data Sharing		Enables interstate data sharing with selected states.
Interstate Data Sharing – Role Management		Allows administrators to enable access rights to selected provider roles for Interstate Data Sharing.
Integration Requests		Displays the request(s) made by Health Care Entities for integration with the state's PDMP system. Allows the PDMP administrator to approve or deny such request(s).
Approve Interstate Data Sharing for Health Care Entities		Allows the PDMP administrator to grant or deny access of health care entities from selected PDMP sites. Only authorized health care entities that have been granted access will be allowed to make prescription report request(s) to a PDMP state.

User Management		Enables PDMP administrators to add new PDMP users.
Provider Validation		Allows PDMP administrators to manage provider validations for Instate/Interstate Request(s) based on the selected DEA/ NPI options. This feature can be disabled by selecting the option “None.”
PDMP Maintenance Schedule		Allows PDMP administrators to create/cancel maintenance schedule request(s).
NCPDP Taxonomy Code Mapping		Displays the available NCPDP taxonomy codes, along with their respective descriptions and PMIX roles.
System Information		Depicts the onboarding status of each U.S. state with the RxCheck system on a U.S. map.

VI. Reporting/Auditing Capabilities

The RxCheck Hub has robust information traceability. The data flows will leave an audit trail that does not include protected health information (PHI) to enable reporting on demand to PDMP administrators. The audit trail includes the requester and identifying site’s contact details (telephone number and email address). The audit trail is not included as part of the transaction; however, it is accessible through the administrator console.

A contract/agreement is required between (1) the state and hub and (2) the state and integration partner(s). All states engaged in data sharing via the RxCheck Hub have signed a memorandum of understanding (MOU) with the IJIS Institute. States may also have agreements with entities within their states that wish to integrate with the state PDMP. The state PDMP should be contacted for information about its procedures.