RxConsole State PDMP Administrator Guide

Version 3.1.2

September 2, 2025

Table of Contents

1. Introduction 5

1.1. Purpose of the RxConsole User Guide 5

1.2. Who is the user guide intended for? 5

1.3. RxConsole Access, Registration, and Authorization 5

2. History and Overview of the RxConsole Application 6

3. Functionality of the RxConsole Application 7

3.1. RxConsole Home Page 8

3.2. User Roles and Privileges in the RxConsole Application 8

4. Getting Started with the RxConsole Application 11

4.1. Open the RxConsole Application 11

4.2. Open the RxConsole Test Site (UAT) Application 12

4.3. Sign in to the RxConsole Application 12

4.4. Reset your mobile authenticator app 14

4.5. Retrieve a forgotten password 16

4.6. Account Timeout and Lockout 16

4.7. Reset the password for your RxConsole Account 17

5. RxCheck Dashboard 18

5.1. Apply filters to the RxCheck Dashboard 18

5.2. View incoming and outgoing requests in the RxCheck Dashboard 21

5.3. Graphical Analysis 22

6. Analytical Insights 24

6.1. View patient and provider prescriptions data in analytical insights 27

7. State Routing Service (SRS) Configuration 30

7.1. Site unique identifier / description 32

7.2 SRS Outbound Sender Endpoint 33

7.3. RxCheck Hub Service Host Endpoint 37

7.4. SRS Inbound Sender Endpoint 37

7.5. Site PDMP Application Endpoint 39

7.6. SRS Certificate 40

7.7. Configure the SRS 41

7.8. Configuring the required fields 42
7.9. Heartbeat and Health Monitoring 43
7.9.1 Current Site Monitoring 43
7.9.2. All Sites Monitoring 45
7.10. Heartbeat notifications 48
8. Hub Audit Logs 50
8.1. Read the hub audit logs 51
8.2. Filter the hub audit logs 53
8.3. Download the hub audit logs 55
8.4. Exporting the logs to an sFTP server 56
8.5. Using an API to download the logs 58
9. Healthcare Entities 59
9.1. Add a new healthcare entity site 60
9.2. Breakdown of Healthcare entity site details 62
9.2.1. Site Details 63
9.2.2. Contact Details 64
9.2.3. Vendor Details 65
9.2.4. Manage Roles 66
9.2.5. Manage Facilities 67
9.2.6. User Administration 70
9.3. Open a healthcare entity record 71
9.4. Export a list of your HCE's and Facilities 72
10. Interstate Data-sharing 75
10.1. Select states for interstate data-sharing 76
10.2. Deselect states for interstate data-sharing 77
10.3. MOU Worksheet(s) 79
10.3.1 Populate and submit the MOU Worksheet 79
10.3.2. Review and respond to an MOU Worksheet submitted to your state 80
11. Interstate Data-sharing – Role Management 82
11.1. Select roles for interstate data-sharing 82
11.2. Deselect roles for interstate data-sharing 84

12. Integration Requests ... 86
12.1. Search for integration requests ... 87
13. Approving interstate data-sharing for healthcare entities ... 89
13.1. Approve or revoke interstate data-sharing requests ... 90
14. User Management ... 93
14.1. Search for and update user information ... 93
14.2. Adding users ... 95
15. Provider Validation ... 96
15.1. View and add a datasource for provider validation ... 96
15.2. View, modify, delete, and search an existing datasource ... 97
15.2.1. Create a datasource file ... 99
15.2.2. Add a new datasource file ... 100
15.2.3. Add a datasource API ... 102
15.3. Configure provider validation options ... 103
15.3.1. Modify an existing provider validation ... 103
15.3.2. Add a new provider validation ... 106
16. PDMP Maintenance Schedule ... 108
16.1. Create and modify a maintenance event ... 108
17. NCPDP Taxonomy Code Mapping ... 113
17.1. Search for an NCPDP Taxonomy Code ... 114
18. System Information ... 115
18.1. Connected PDMP Sites ... 117
19. System Notifications ... 118
20. Exit the RxConsole application ... 119
21. Contact the RxCheck Team ... 120
22. Version History Log ... 121
23. Appendix ... 122

1. Introduction

1.1. Purpose of the RxConsole User Guide

This guide is designed to assist state Prescription Drug Monitoring Program (PDMP) administrators in effectively using the RxConsole application to manage their state's settings within the RxCheck Hub. It provides comprehensive, sectioned instructions covering each feature and function of RxConsole application. Each section includes step-by-step procedures and visual documentation to support accurate and efficient use of the application.

1.2. Who is the user guide intended for?

This user guide is intended for all stakeholders using version 3.1.2 of the RxConsole application on Windows and Mac platforms. Its primary audience includes state PDMP administrators and authorized staff members who have access to the RxCheck interstate network. It is also a valuable resource for personnel assigned to use RxCheck for the first time.

The guide is structured to support both new and experienced PDMP administrators, offering clear instructions to ensure effective use of RxConsole's features and functionalities.

1.3. RxConsole Access, Registration, and Authorization

The Integrated Justice Information Systems (IJIS) Institute is the designated administrator of the RxCheck hub and the RxConsole application.

The Prescription Drug Monitoring Program Training and Technical Assistance Center (PDMP TTAC) maintains official records of each state's PDMP profile, including administrative contact information such as the designated PDMP Administrator, Director, or Manager. These individuals, as identified by PDMP TTAC, hold primary authority to request, assign, delegate, or authorize access to the RxConsole application.

Only those designated by PDMP TTAC may be granted the PDMP Admin user role. This role provides administrative-level access to RxConsole and is created by the RxCheck administrator upon authorization. Only the PDMP TTAC-identified primary PDMP Administrator(s) are permitted to add, modify, activate, or deactivate PDMP Admin user accounts. If you are a PDMP administrator and do not have access to the RxConsole application, please contact the RxCheck Team as described in the section titled, *Contact the RxCheck Team* near the end of this guide.

2. History and Overview of the RxConsole Application

The RxConsole application is the management console for the RxCheck Hub. The RxCheck Hub facilitates interstate data-sharing between state PDMPs. This means a state only needs to establish one connection to the hub to share data with all other participating states. Beyond data sharing, the hub also provides a method for healthcare entities to connect to their respective PDMPs and offers states a centralized solution for managing these connections. It's important to note that the RxCheck Interstate Data Sharing Hub is not a PDMP itself. Instead, it offers a wide range of services to PDMPs looking to engage in data sharing with PDMPs in other states.

The RxCheck Interstate Hub was established with support from the U.S. Bureau of Justice Assistance (BJA) and the Centers for Disease Control and Prevention (CDC) to provide a secure, cost-free, and standardized method for interstate sharing of prescription drug data. Operated by BJA and administered by the RxCheck Advisory Body—comprised of PDMP representatives from participating states and territories—RxCheck is the only federally designated, non-proprietary platform for PDMP data exchange. It supports integration with electronic health record (EHR) systems, pharmacy management systems, and health information exchanges (HIEs), thereby improving nationwide access to PDMP data.

RxCheck was developed to address critical challenges in combating the opioid epidemic, such as the lack of cross-state visibility into patients' prescription histories. Without a unified system, prescription abusers have been able to obtain multiple prescriptions across state lines undetected, limiting the ability of healthcare providers to make informed prescribing decisions. RxCheck enhances data transparency, preserves state ownership of PDMP data, and eliminates financial and technological barriers associated with proprietary solutions.

The initiative began in 2005 when BJA partnered with the Integrated Justice Information Systems (IJIS) Institute—a nonprofit focused on public sector technology—to explore solutions for interstate data sharing. This led to the formation of the BJA/IJIS PDMP Committee, which included state PDMP administrators, federal staff, and IJIS representatives. The effort culminated in the creation of the Prescription Monitoring Information Exchange (PMIX), a standardized framework and hub for interstate PDMP data exchange. Over time, this evolved into the RxCheck Hub, which now operates as version 3.1.2.

RxConsole enhances this infrastructure by offering an array of administrative tools and capabilities. These features collectively support the secure, efficient, and scalable exchange of controlled substance prescription data across jurisdictions.

3. Functionality of the RxConsole Application

RxConsole provides PDMP administrators and authorized users with a comprehensive set of tools to manage and monitor prescription data sharing activities within the RxCheck interstate network. The following high-level functionalities are available through the RxConsole interface:

RxCheck Dashboard Monitoring

- View a summary of all incoming and outgoing prescription requests associated with your PDMP on the RxCheck Dashboard.

Analytical Insights

- Generate and view anonymized prescription analytics by patient or prescriber, with filtering options by county and ZIP code.

State Routing Service (SRS) Configuration

- Set up and manage State Routing Service parameters for data transmission and routing.
- Establish heartbeat and health monitoring and notifications for site connectivity and IT diagnostics.

Hub Audit Logs

- Access, filter, and export comprehensive Hub Audit Logs detailing data transaction activities.

Health Care Entity (HCE) Management

- Create and manage HCE site profiles.
- Define and manage user roles associated with each HCE.
- Configure and manage HIE subsite facilities under each HCE.

Interstate Data Sharing Control

- Grant or revoke access to HCE sites for interstate data exchange.
- Manage roles and permissions for interstate sharing.

Interstate Data Sharing Role Management

- Manage roles and permissions for interstate sharing.

Integration Request Management

- Review and approve or deny integration requests submitted by HCEs seeking connectivity.

Interstate Data Sharing Request Management

- Review and approve or deny requests from HCEs to share data across state lines.

PDMP User Management

- Administer PDMP user accounts and manage user-specific settings.

Provider Validation Management

- Configure validation settings for providers using DEA numbers, National Provider Identifiers (NPI), and state license numbers.

Maintenance Scheduling

- Create, monitor, and track system maintenance events.

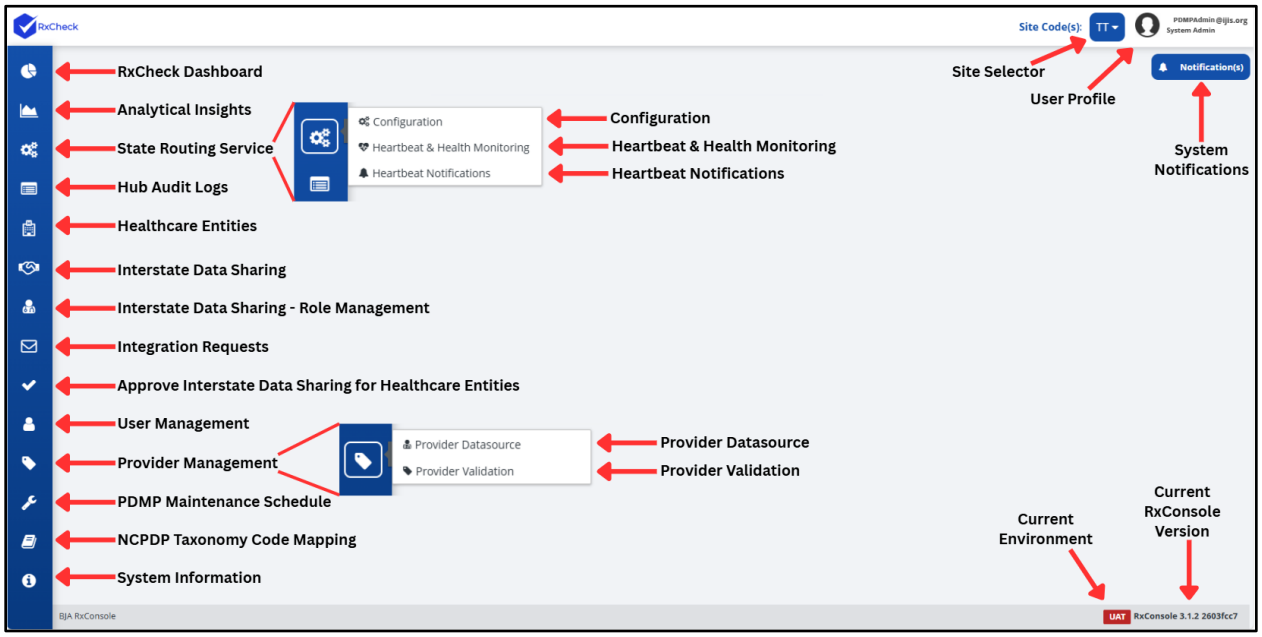
Taxonomy Code Search

- Search and view mappings related to the NCPDP Taxonomy Code.

System Status Monitoring

- View system information and connectivity status for all integrated PDMP sites.

3.1. RxConsole Home Page



3.2. User Roles and Privileges in the RxConsole Application

The RxConsole provides the minimum necessary privileges needed to perform their work to the individuals accessing the application. This differentiation is achieved with user roles. Within RxConsole, there are 4 main user roles:

- SUPER_ADMIN *Only available to the developers of the RxCheck system.
- ADMIN
- SUB_ADMIN
- USER

Note: SUPER_ADMIN information is included for informational purposes only.

The ADMIN role can be further broken down into 2 sub-roles:

- **State—**State employees or contractors with a state email address.
- **Vendor—**Company responsible for overseeing the management of the PDMP software.

The tables below outlines the privileges by user role in the RxConsole application.

RxCheck Console Module	ADMIN - State	ADMIN - Vendor	SUB_ADMIN	USER
RxCheck Dashboard	**X**	**X**	**-**	**-**
Analytical Insights	**X**	**-**	**-**	**-**
State Routing Service	**X**	**X**	**X**	**-**
Hub Audit Logs	**X**	**X**	**X**	**X**
Healthcare Entities	**X**	**X (view-only)**	**-**	**-**
Interstate Data Sharing	**X**	**X**	**-**	**-**
Interstate Data Sharing—Role Management	**X**	**X**	**-**	**-**
Integration Requests	**X**	**-**	**-**	**-**
Approve Interstate Data Sharing for Healthcare Entities	**X**	**-**	**-**	**-**
User Management	**X**	**-**	**-**	**-**
Provider Management	**X**	**-**	**-**	**-**
PDMP Maintenance Schedule	**X**	**X**	**-**	**-**
NCPDP Taxonomy Code Mapping	**X**	**X**	**X**	**X**
System Information	**X**	**X**	**X**	**X**

A SUPER_ADMIN account is like the ADMIN-STATE role in that it has access to all the RxCheck Modules and is only available to the RxCheck system developers. Additionally, the SUPER_ADMIN role has the following privileges not available within the RxConsole Modules:

- Manage State connections and HCE's
- Manage PMIX roles
- Manage Bridge Connections (FEDERAL, STATE, HUB2HUB, MULTI-STATE-HCE)
- Manage provider data for the state
- Manage push notifications
- View the state's usage dashboard
- Access to interstate data-sharing for a state for debugging
- Access to interstate role management for a state for debugging

- Integration requests received for a state
- User management – only for creating PDMP Administrators
- Admin Configuration – real-time connection status monitoring, versions, sync protocol versions, jvm parms
- NCPDP Taxonomy Code Mapping
- System Information
- User lookup and password change
- Activity logs

4. Getting Started with the RxConsole Application

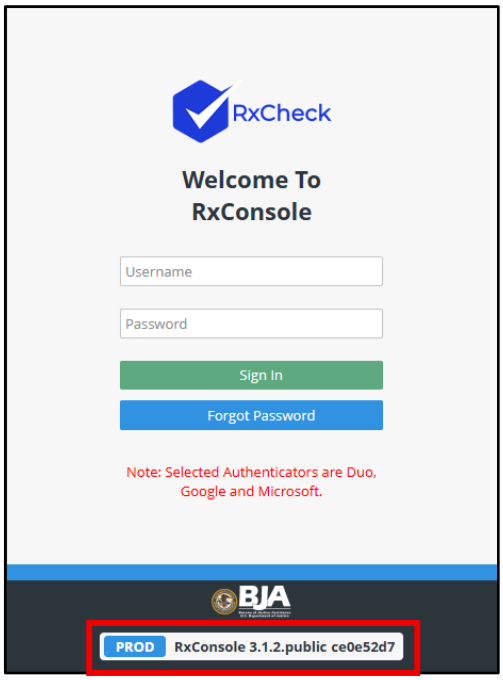
This section provides step-by-step instructions for accessing the RxConsole application. Each step is supported by visual aids, such as screenshots, to ensure clarity and accuracy throughout the process.

Note: RxCheck operates two distinct environments: **Production** and **Test (UAT)**.
Access to each environment is determined by the specific URL used. The URL will indicate if you are connected to the test or production site and the login page displays the current application version at the bottom right of the page.

4.1. Open the RxConsole Application

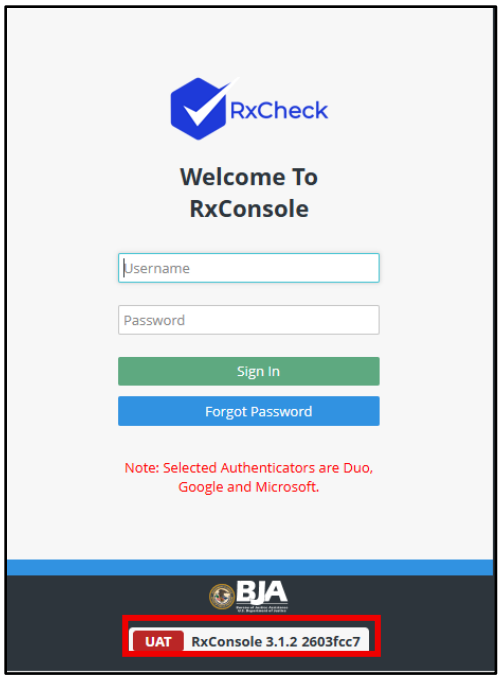
1. Navigate to the following URL in your internet browser bar: https://console.rxcheck.org/rxconsole/#/login

   Note: At the bottom of the page, there is text indicating the site type is production "(PROD)", along with the RxConsole version number.



4.2. Open the RxConsole Test Site (UAT) Application

1. Navigate to the following URL in your internet browser bar to load the RxConsole Login page: https://test.rxcheck.org:18803/tetrus-rxcheck/#/login



Note: At the bottom of the page, there is text indicating the site type is Test "(UAT)", along with the RxConsole version number.

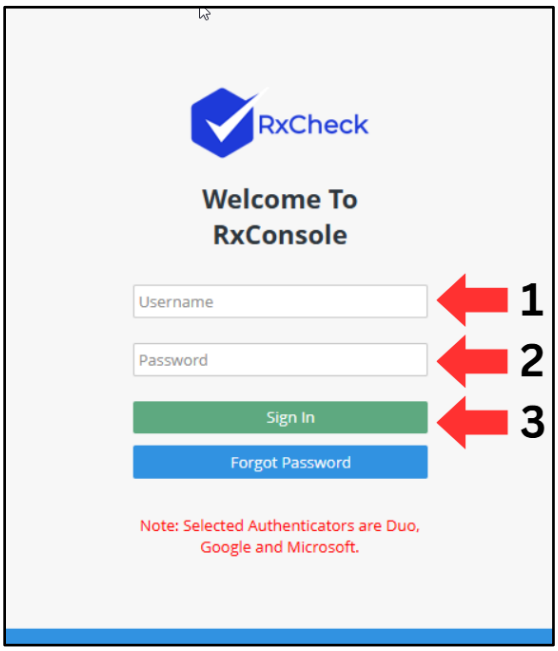
4.3. Sign in to the RxConsole Application

Personal login credentials are required to log into the RxConsole application. Login credentials will be provided to the state PDMP administrators during the onboarding process. **For further inquiries regarding your login credentials, please contact the RxCheck help desk as described in the *Contact the RxCheck Team* section.**

1. Enter your RxCheck username in the first text box.

2. Enter your RxCheck Password in the second text box.

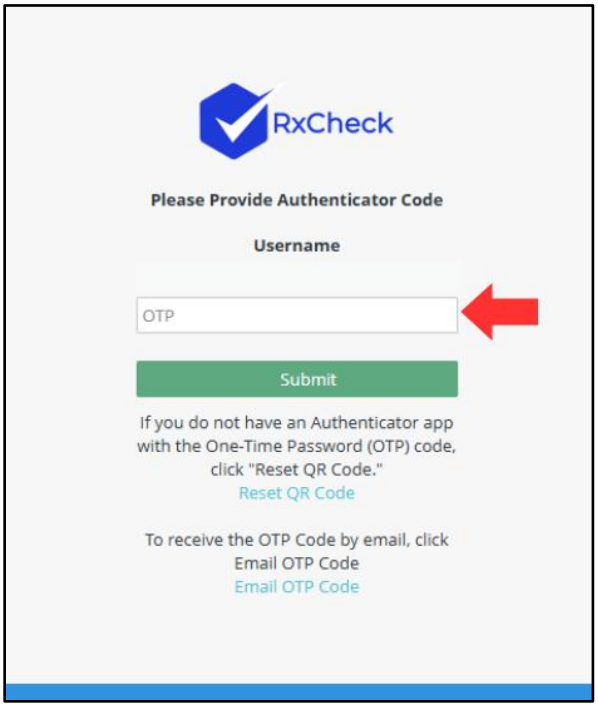
3. Click on the *Sign In* button.



4. Users can receive the one time password (OTP) two ways:
   a. Click *Email OTP Code* on the login screen to have the code sent to their login email.
   b. Use one of the three approved authenticator apps to generate the OTP on their mobile device.

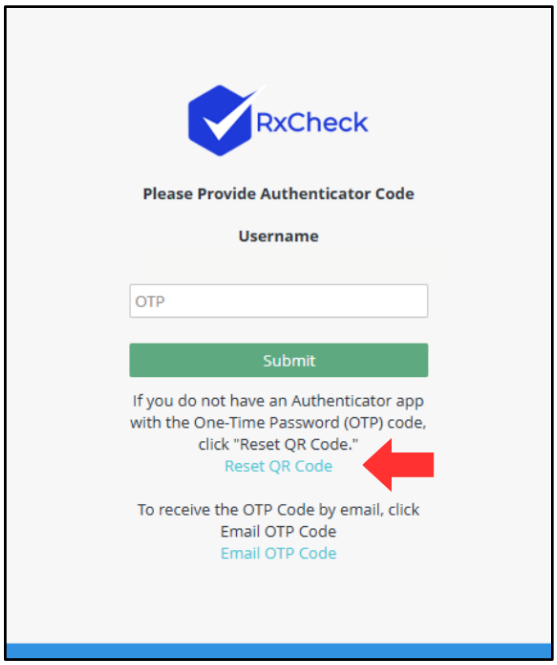
5. To view the OTP code on a mobile device, install **Google, Microsoft, or Duo Authenticator** from:
   a. The **Play Store** (Android)
   b. The **App Store** (iPhone)

6. Enter the OTP code from the email or authenticator app and click on the *Submit* button.

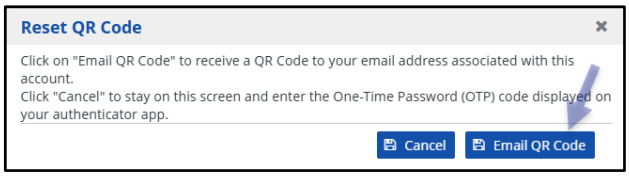


4.4. Reset your mobile authenticator app

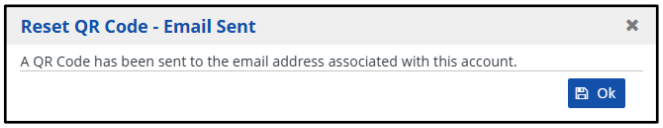
1. Users can set up or reset their authenticator app by:
   a. Scanning the QR code from their RxConsole account creation email, or
   b. Clicking *Reset QR Code* on the authenticator code screen



2. If you clicked the *Reset QR Code* link, press the *Email QR Code* button on the following screen.

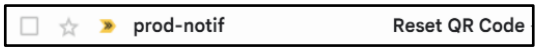


3. A *Reset QR Code – Email Sent* pop-up will display.



4. Press the *Ok* button.

5. Users will receive an email from "prod-notif" with the subject **Reset QR Code**.



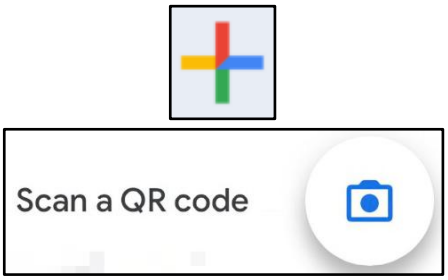
6. Open the email and scan the QR Code.

   Note: *the QR code here is for reference only.*

Note: If the user previously set up authentication in a mobile authenticator app, they should delete the existing RxConsole account entry in that authenticator app before scanning the new QR code to avoid duplicate entries.

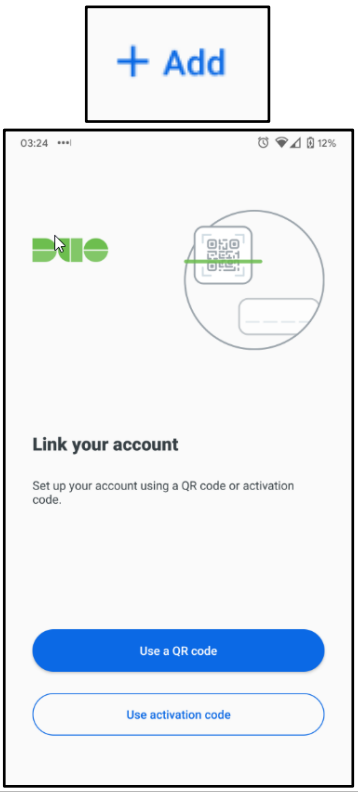
Set up using Google Authenticator app

1. Launch the Google Authenticator app on your mobile device.
2. Press the **+** button.
3. Press the camera icon to scan a QR code.
4. Scan the QR code in the RxConsole email.



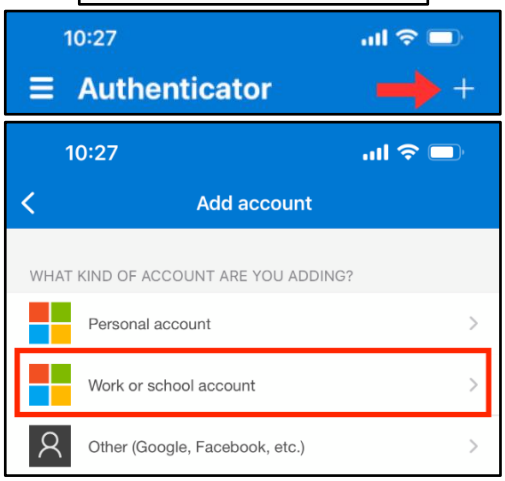
Set up using Duo Mobile Authenticator app

1. Launch the Duo Mobile Authenticator app on your mobile device.
2. Press the **+ Add** button.
3. Press the **Use QR Code** button.
4. Scan the QR code in the RxConsole email.



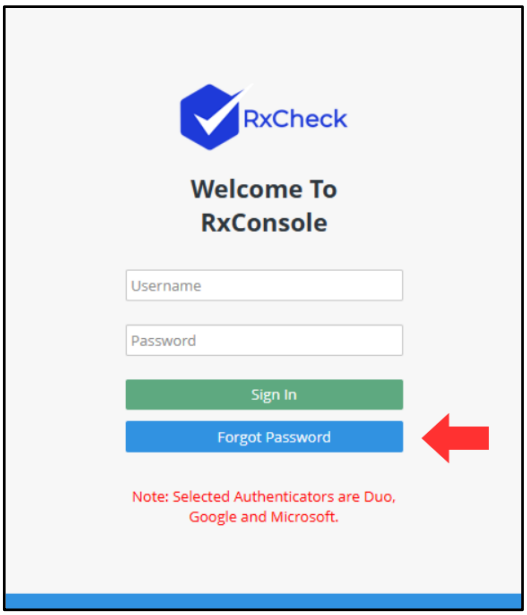
Set up using Microsoft Authenticator app

1. Launch the Microsoft Authenticator app on your mobile device.
2. Press the **+** icon.
3. Select *Work or school account*.
4. Press the *Scan QR Code* option.
5. Scan the QR code in the RxConsole email.

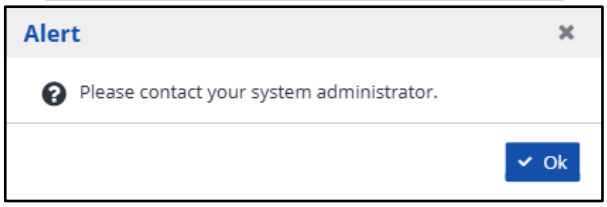


4.5. Retrieve a forgotten password

1. Click on the *Forgot Password* button.



2. An *Alert* pop-up will display: "Please contact your system administrator."



Note: Users must ***send the password update request from the email address they use to log into the RxConsole application*** to the RxConsole support team.

4.6. Account Timeout and Lockout

The RxConsole application includes security features designed to assist with account security and may be triggered during routine use of the system.

Timeout—All RxConsole roles will experience a 15-minute period in which they will not be able to access the RxConsole application after five (5) failed password attempts. After the 15-minute timeout period, the password attempts will reset.

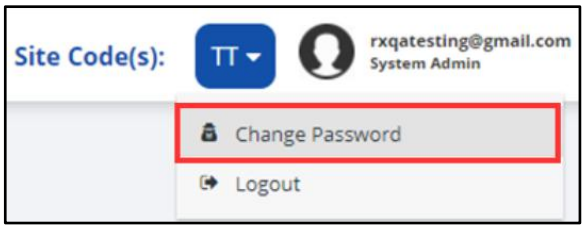
Lockout—All RxConsole roles should automatically inactivate after a user has been inactive for 180 consecutive days. To reactivate the account, the user will need to reach out to the RxCheck Support Team.

4.7. Reset the password for your RxConsole Account

Users can change their password for security purposes or other reasons by following the instructions below. It is recommended that your password be updated every 30 days for increased account security.

1. Click on your username on the top right-hand corner of the screen.

2. Select the *Change Password* dropdown option.



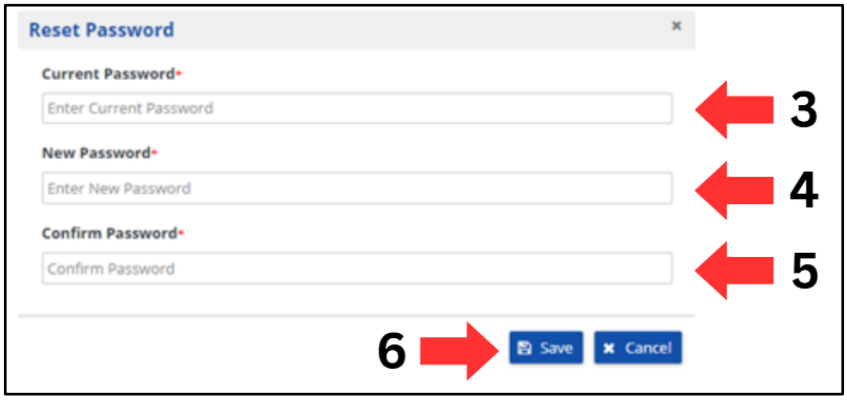
3. Enter your current password in the "Current Password" box.

4. Enter your new password in the "New Password" box.

5. Re-enter your new password in the "Confirm Password" Box.

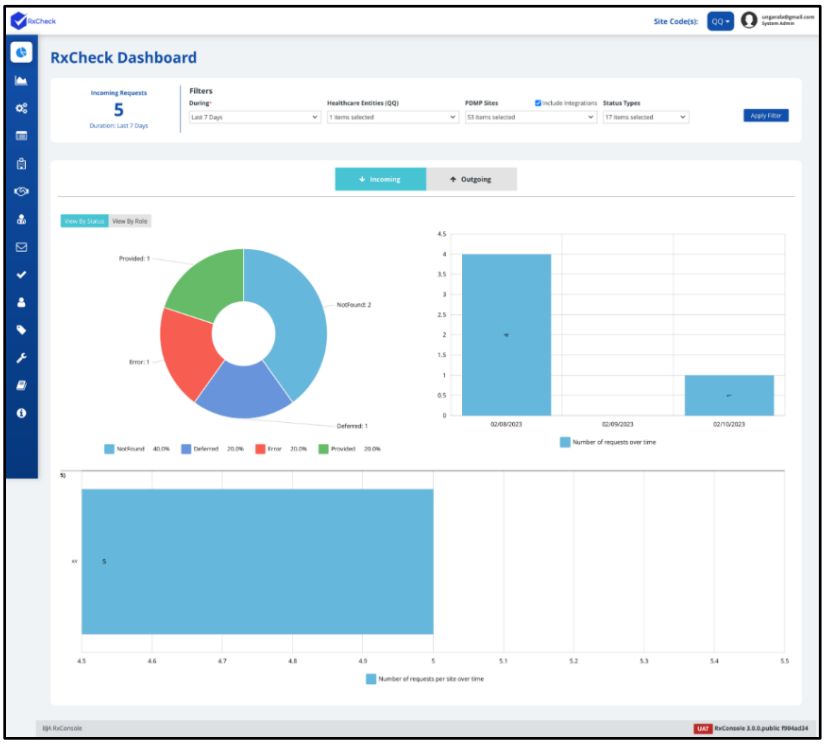
   Note: This ensures the user enters the new password as intended.

6. Click on the *Save* button to implement the password change.



5. RxCheck Dashboard

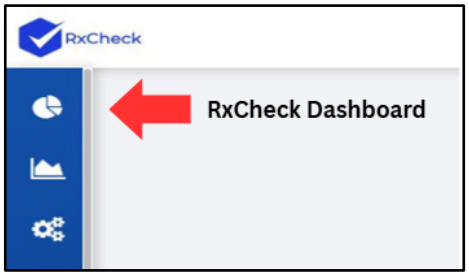
The RxCheck Dashboard provides a location for PDMP administrators and other authorized users to view metrics on their state's RxCheck usage.



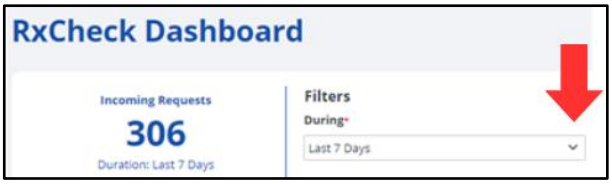
Note: The RxCheck Dashboard will only work after the PDMP SRS is configured. Information regarding the SRS (State Routing Service) including where to download the software can be found in the section titled, *State Routing Service (SRS) Configuration*.

5.1. Apply filters to the RxCheck Dashboard

1. Click the pie graph icon on the left-hand side of the screen to access the RxCheck Dashboard.

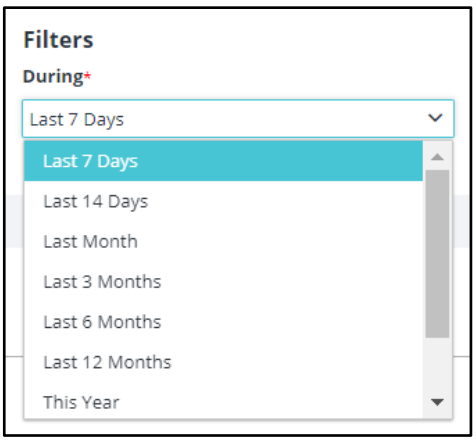


2. Click on the downward-facing arrow for the filter titled "During" to reveal options to filter by.

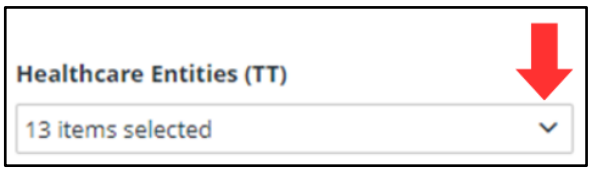


3. Select the period to match the historical timeframe you would like to populate the RxCheck dashboard.

   ***Note*:** This filter is set to last 7 days by default.

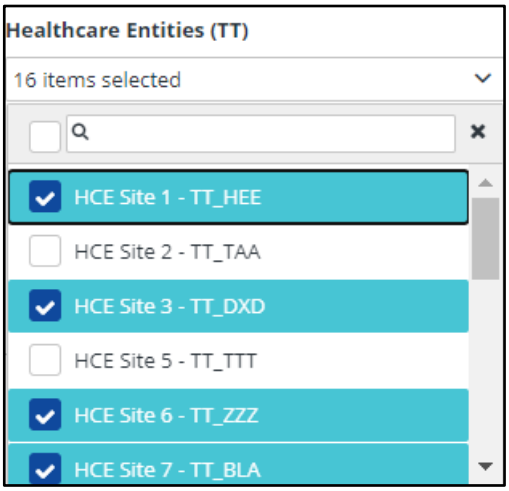


4. Click on the downward-facing arrow for the filter titled "Healthcare Entities (PDMP-Site Code)" to reveal a list of healthcare entities.

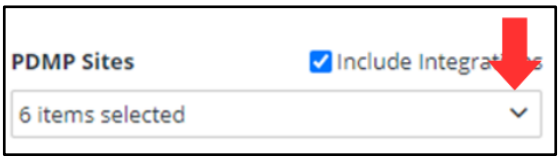


5. Select the desired healthcare entity(ies) by:
   a. Scrolling through the dropdown and checking the box next to each desired entity, or
   b. Typing in the **Search Bar** to filter the entities.

   ***Note*:** By default, all options are selected. To clear your selections, click the checkbox next to the search bar before choosing your desired options.

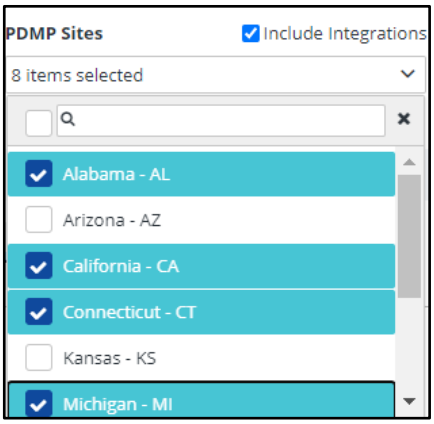


6. Click on the downward-facing arrow for the filter titled "PDMP Sites" to reveal a list of states.



7. Select the desired PDMP Site(s) by:
   a. Scrolling through the dropdown and checking the box next to each desired state, or
   b. Typing in the **Search Bar** to filter the states.

   Note: By default, all options are selected. To clear your selections, click the checkbox next to the search bar before choosing your desired options.



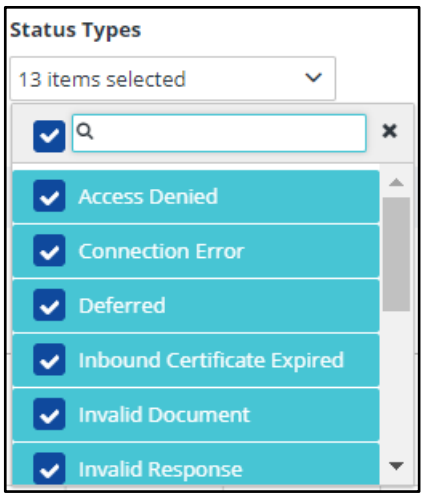
8. Uncheck the "Include Integrations" box to exclude transaction counts from out-of-state healthcare entities.

   Note: This option is selected by default.

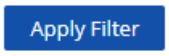
9. Click on the downward-facing arrow for the filter titled "Status Types" to reveal a list of status options.

10. Select the desired Status Type(s) by:
    a. Scrolling through the dropdown and checking the box next to each desired status, or
    b. Typing in the **Search Bar** to filter the status types.

    Note: By default, all options are selected. To clear your selections, click the checkbox next to the search bar before choosing your desired options.



11. Click on the *Apply Filter* button to apply your selected filters on the dashboard.



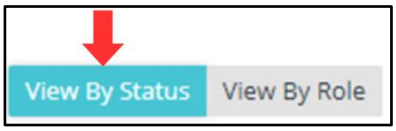
5.2. View incoming and outgoing requests in the RxCheck Dashboard

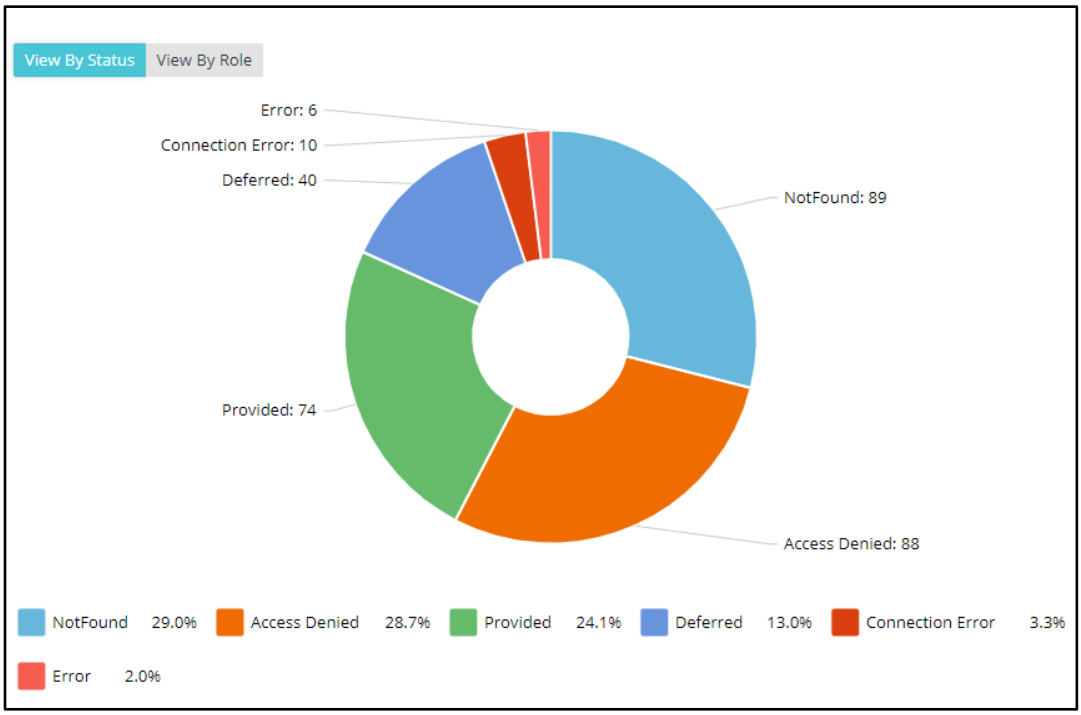
1. Click on either the *Incoming* or *Outgoing* button located below the filters on the RxCheck Dashboard screen. This will allow you to view the selected requests.

   Note: The *Incoming* option is selected and displayed by default.

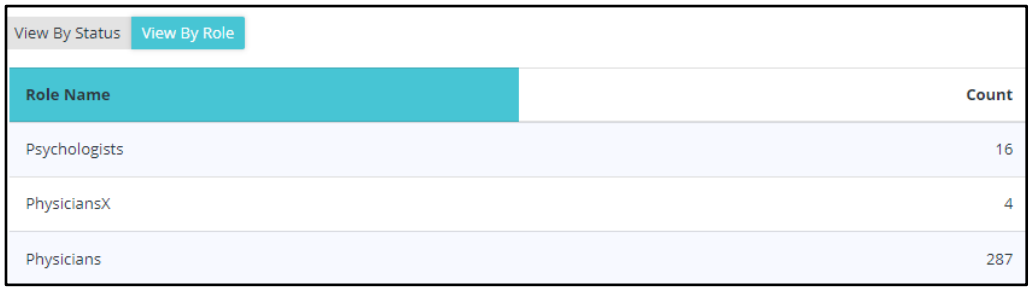
2. Perform the steps from the "[Apply filters to the RxCheck Dashboard](#)" section of this guide.

3. Select the *View by Status* button to view a graphical representation of the data, based on the status.



4. Select the *View by Role* button to view the total count of requests made by professionals in a certain role.



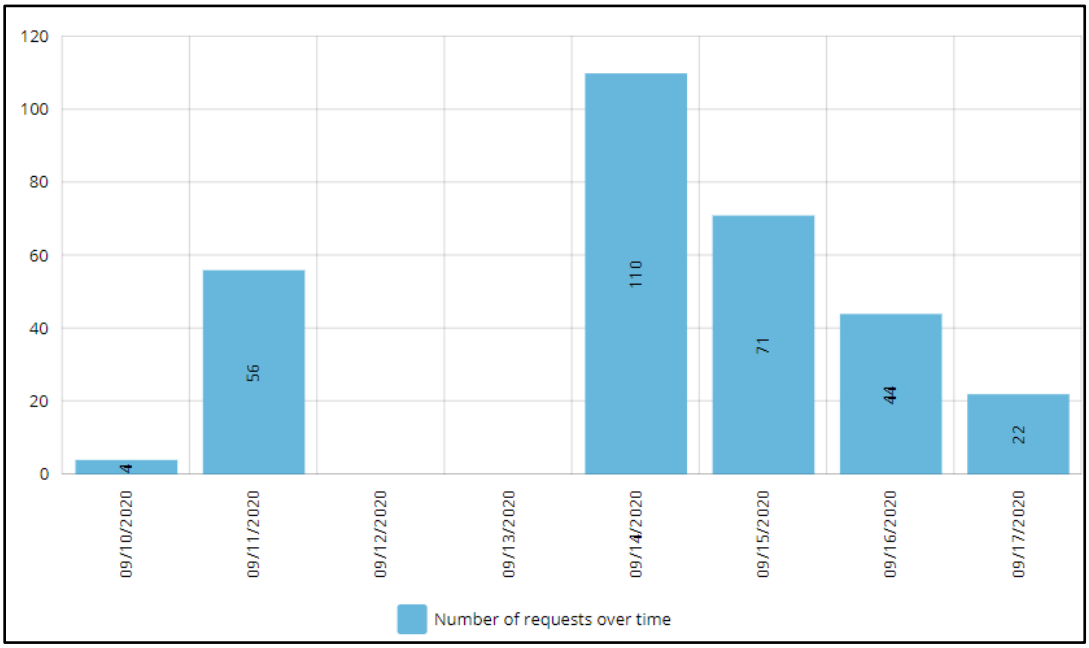
Role Name	Count
Psychologists	16
PhysiciansX	4
Physicians	287

Note: The steps are the same between incoming and outgoing requests.

5.3. Graphical Analysis

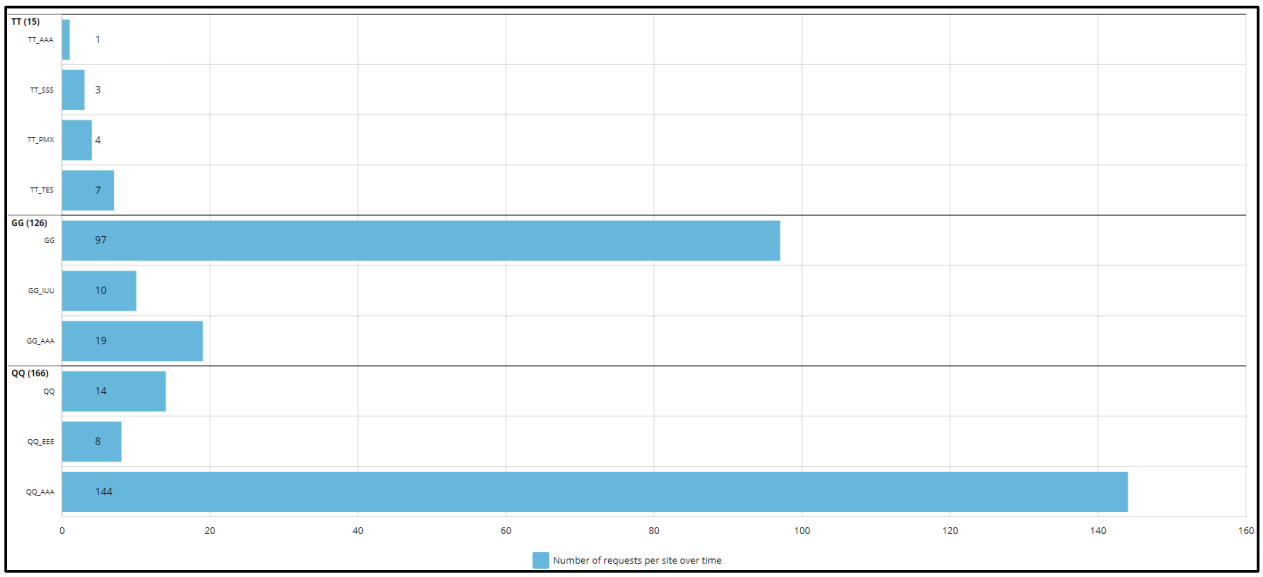
The following bar graph depicts the distribution of requests over time, matching your selected dashboard filters.

The Y-axis represents the number of requests, while the X-axis represents the time frame. The blue bars represent the request volume over time.



The following horizontal bar graph depicts the number of requests from site(s) over time, matching your selected dashboard filters.

The Y-axis represents the site(s) in the PDMP user's state, while the X-axis represents the volume of requests. The blue bars represent the distribution of request volume per site in the time period selected in the dashboard filters.

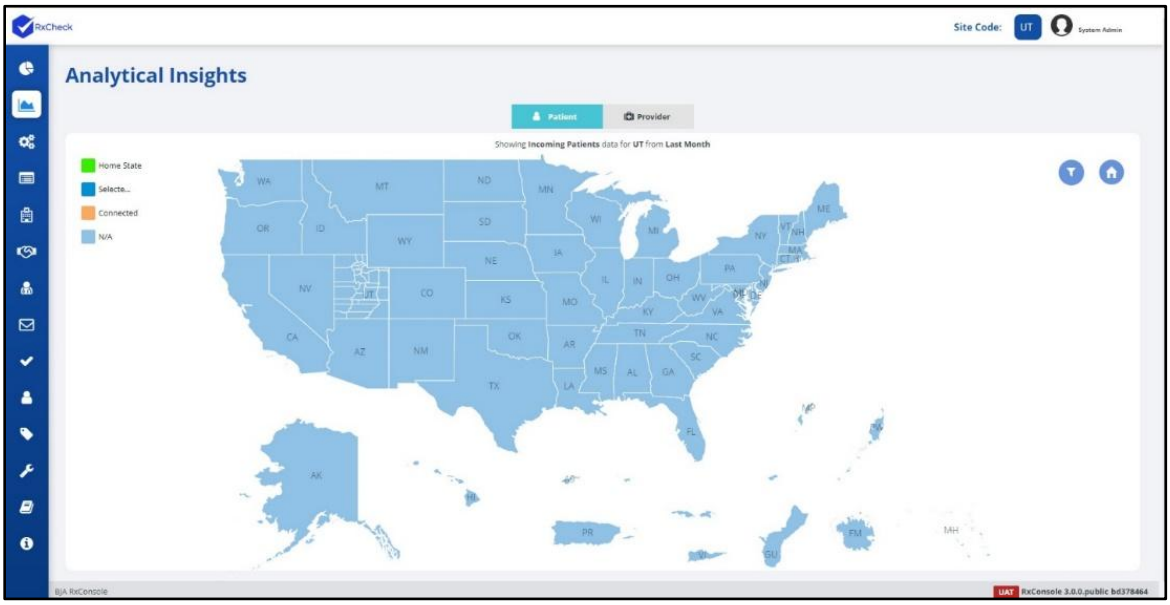


6. Analytical Insights

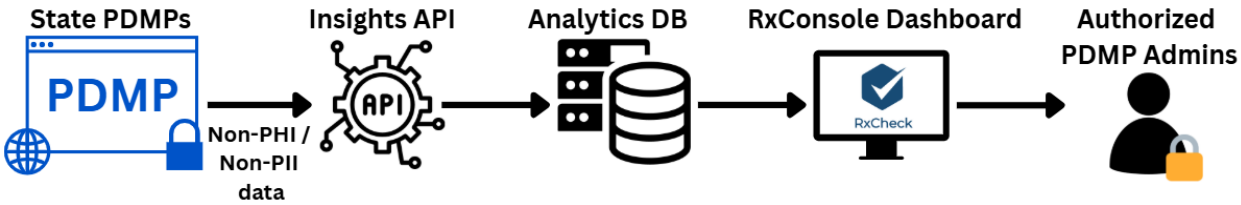
The Analytical Insights dashboard allows each state to analyze prescription trends and patterns at a high level. It provides visibility into how prescriptions from other states are being dispensed within the state, as well as how the state's own prescriptions are being filled outside its borders. This feature supports the identification of individuals traveling from other states to fill prescriptions and highlights out-of-state pharmacies dispensing prescriptions written in the user's state.

It is important to note that all posted data and visualizations are based on:

- Aggregate data
- Anonymized data
- No PHI or PII data is disclosed



For the Analytical Insights dashboard to function in the RxConsole, a state will need to send Non-PHI and Non-PII data to the Insights API, where it can then be added to the database and displayed within the RxConsole.



A state PDMP Administrator wishing to participate in this module, will need to submit data to the RxCheck Team. This data should be free of PHI and PII before being submitted. The following data is required for the Analytical Insights dashboard to begin functioning:

- The month for which the data is submitted
- The PDMP that is posting the data
- Zip code, county, or state from where the prescriptions were dispensed
- Total number of dispenses by zip code, county, or state
- Total number of out-of-state dispenses (for patients and/or providers) by the zip code, county, or state
- Total number of providers, patients, and prescriptions

Some information to keep in mind regarding the Analytical Insights Feature:

- A state's participation is voluntary
- Data does **not** contain PHI or PII
- Access is limited to authorized PDMP staff members from a participating PDMP and Tetra Ventures for system administration
- The PDMP controls their data and determines:
  - Level of detail (Rx general location information) for the data
  - Which other PDMPs to engage
- No cost is imposed to participate or use this tool
- Free assistance is available to develop the data file
- If desired, a state can request a user agreement for this tool detailing access and use parameters for PDMPs

Below, there is an example for a submission for provider information submitted from Kentucky (sample data).


```
{
	"PDMPAnalyticsData": {
		"FilledDate": "03/17/2023",
		"PublishState": "KY",
		"DispenseDataByZip": {
			"dispenseZip": "41008",
			"totalDispense": "100",
			"totalOutofStateDispense": "5",
			"ProvidersFilledFromOutState": [
				{
					"filledStateCode": "WV",
					"filledFromZip": "24712",
					"totalProviders": "2",
					"totalPrescriptions": "3"
				}, {
					"filledStateCode": "TN",
					"filledFromZip": "37011",
					 "totalProviders": "1",
					"totalPrescriptions": "1"
				}, {
					"filledStateCode": "IN",
					"filledFromZip": "46077",
					 "totalProviders": "1",
					"totalPrescriptions": "1"
				}
			]
		}
	}
}
```

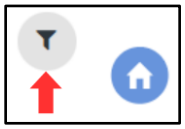

After data has been submitted, the map should begin to populate in the Analytical Insights module within RxConsole.

6.1. View patient and provider prescriptions data in analytical insights

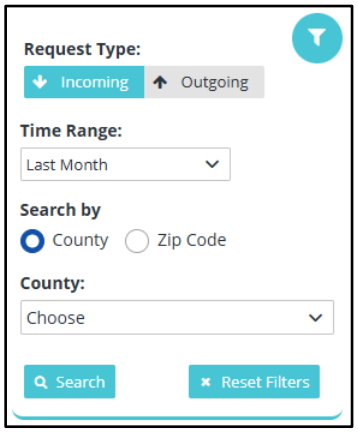
1. Click the area graph icon on the left-hand side of the screen to access the RxCheck Dashboard.

2. Click on the *Patient* or *Provider* button located in the top middle of the page, depending on the information you would like to display.

3. Click on the filter button in the top right corner.

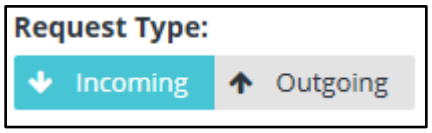


4. After clicking the filter button, you can view the search filters.

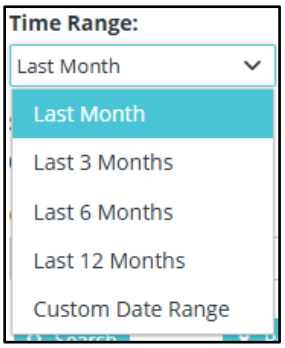


5. The *Incoming* and *Outgoing* buttons allow you to filter the request type.

   Note: The *Incoming* option is selected and displayed by default.



6. Use the *Time Range* dropdown to select a period you want to display.

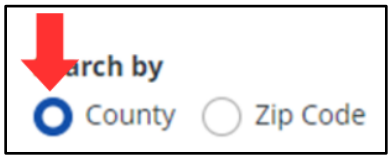


7. Prescription information can be searched by *County* or *Zip Code.*

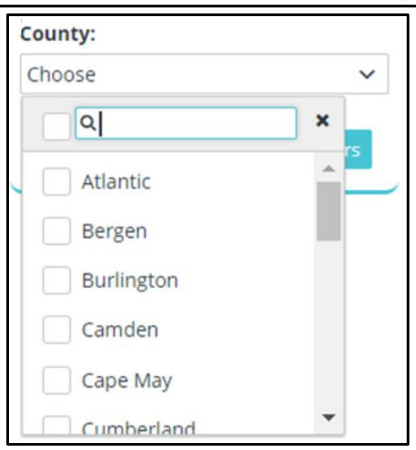
How to search by county

1. Click on the *County* radio button.

   Note: The *County* button is selected by default.



2. Click on the downward-facing arrow for the filter titled "County" to reveal a list of counties.



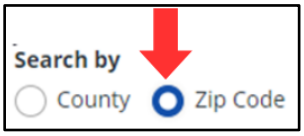
3. Select your County(ies) by:
   a. Scrolling through the dropdown options and checking the box, or
   b. Typing in the search bar to filter results.

4. Click the *Search* button to display prescription counts for patients based on the counties selected.

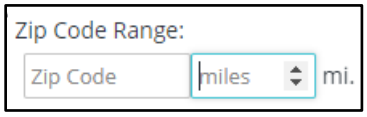
5. Results are displayed on the map with the user's state highlighted green and the connected states in orange.

How to search by Zip Code

1. Click on the *Zip Code* radio button.



2. Enter the zip code and the desired distance in miles around the zip code to be searched.



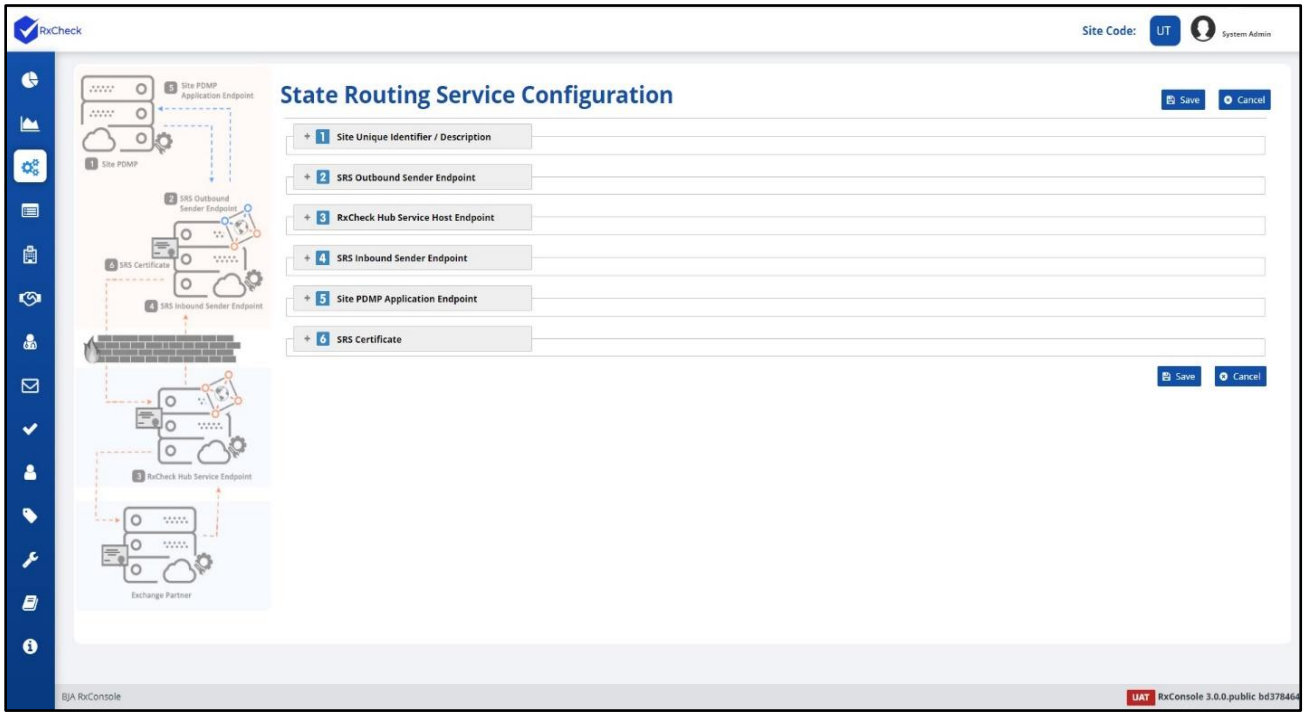
3. Click the *Search* button to display prescription counts for patients based on the zip code and range entered.

4. Results are displayed on the map with the user's state highlighted green and the connected states in orange.

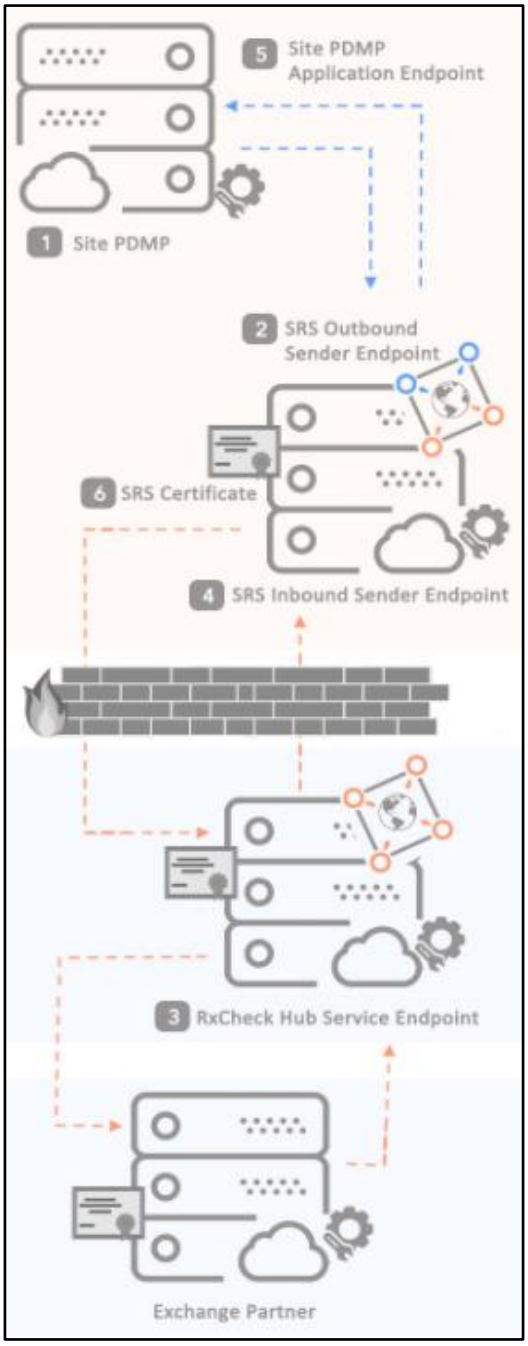
Note: Click on the *Reset Filters* button to return all selections to the default values.

7. State Routing Service (SRS) Configuration

Every state PDMP officially onboarded into the RxCheck system will have a routing service installed that allows it to send and receive messages from other states. Message content between states is encrypted for privacy and security purposes and can only be accessed and decrypted by the state intended to receive the message.



Note: If your state does not have an SRS currently installed, one will need to be installed before connecting to the RxCheck Hub. While you can log into the RxConsole application, some functionality will not work without the PDMP connected. The latest SRS installation files can be found here: https://rx-check.org/Hub/ConnectionTools.



One of the initial responsibilities assigned to a State PDMP Admin is the configuration of their State Routing Service (SRS). The State Routing Service is a software that facilitates the successful transmission of messages between Health Care Entities and PDMP states. Configuring the SRS is a six-step process, and each of these steps is listed below, as well as graphically depicted in the diagram on the left.

To configure the State Routing Service, the State PDMP Admin will need to enter the requested information into the data fields present under each section of the State Routing Service Configuration page. A detailed explanation of each section and its corresponding data fields are provided below.

State Routing Service Configuration Process for a PDMP State:

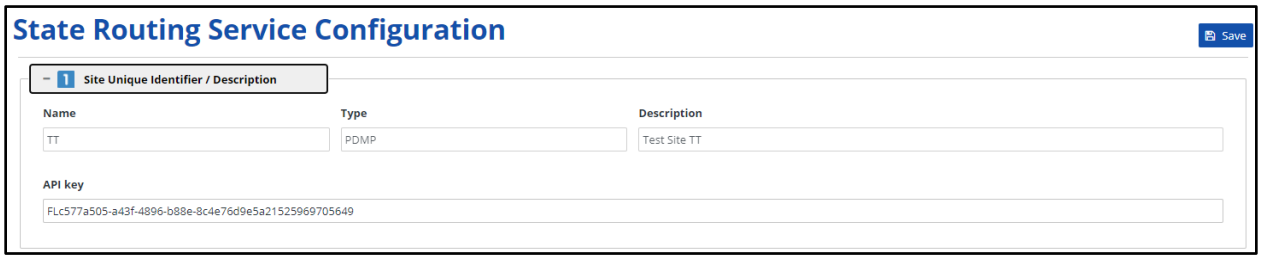
1. Site Unique Identifier/ Description.
2. SRS Outbound Sender Endpoint.
3. RxCheck Hub Service Host Endpoint.
4. SRS Inbound Sender Endpoint.
5. Site PDMP Application Endpoint.
6. SRS Certificate.

The following subsections contain instructions on how to configure the State Routing Service in the RxConsole application. For additional clarity, each step is accompanied by a corresponding image or screenshot that depicts the action described.

7.1. Site unique identifier / description

This section covers general information about the site for which the SRS is to be configured. All data fields in this section are auto-populated based on the data that was entered by the Super Administrator when the site was initially created. The State Admin users can review the auto-populated data in this section and contact the RxCheck technical team if there are any questions or concerns.

The following screenshot depicts the configuration process for the Site Unique Identifier/ Description section. For additional clarity, the ensuing table provides a definition of each data field present in the screenshot.



Data Field Name	Description
Name	The official two-letter state abbreviation code assigned to each state. E.g., New Jersey: NJ, California: CA ***This field is auto-populated.***
Type	The Site Type assigned to each state is PDMP (Prescription Drug Monitoring Program). ***This field is auto-populated.***
Description	A brief description of the site. ***This field is auto-populated.***
API Key	An Application Programming Interface (API) key serves as a unique identifier for the site and is generated when the site is created. The first two letters of an API key will always represent the Name of the site. It is a security key that is validated for SRS connections. ***This field is auto-populated.***

7.2 SRS Outbound Sender Endpoint

This section enlists the standards and interfaces that are supported by the RxCheck application for all request and response transactions. This step allows State PDMP Administrators to select/enter specific details pertaining to their unique PDMP site environment.

Currently, RxConsole supports the following interfaces:

- PMIX/NIEM – National Information Exchange Model
- NCPDP 2017 – National Council for Prescription Drug Programs
- HL7 FHIR – Health Level Seven International (HL7) Fast Healthcare Interoperability Resources (FHIR)
- HTML5 – Hypertext Markup Language 5

A brief description of each type of interface is listed below:

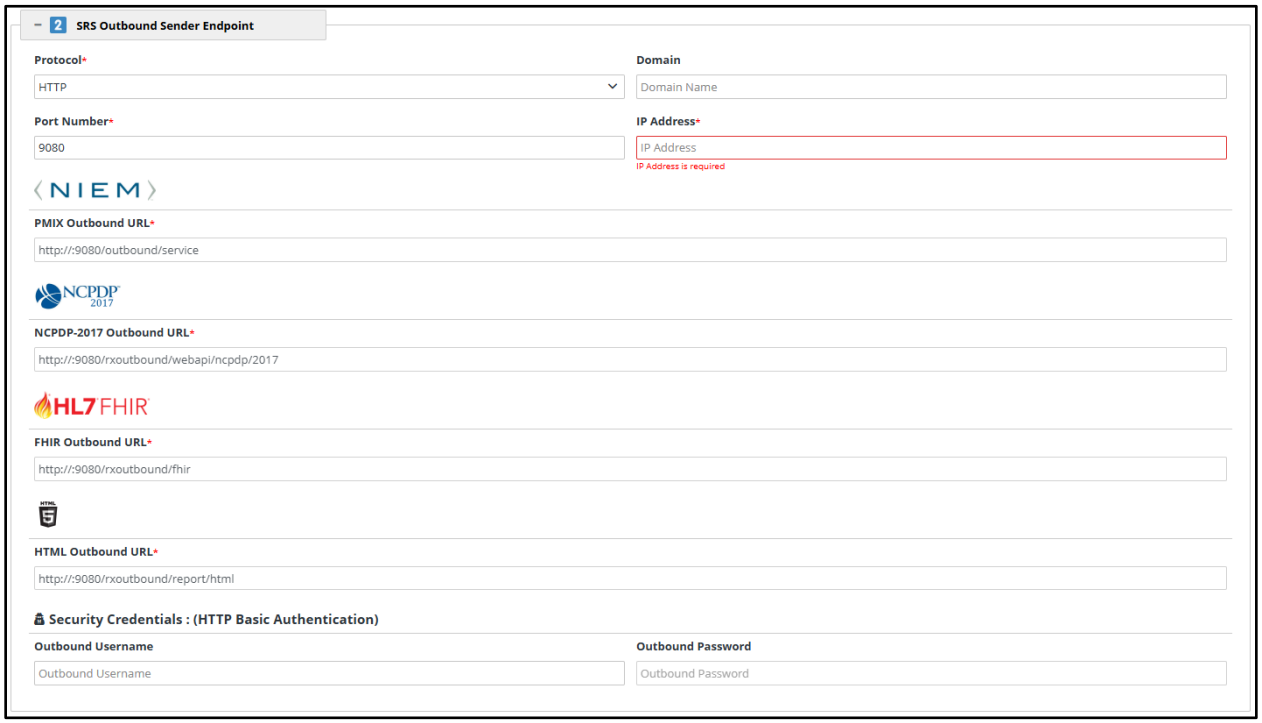
- **PMIX:** The PMIX Standards Organization supports the sharing of Prescription Drug Monitoring (PDMP) program Data among PDMP organizations and their stakeholders by establishing and maintaining the PMIX National Architecture and related guidelines, policies and standards to minimize the cost and complexity of sharing PDMP data across organizational, vendor, geographic and operational boundaries; enable secure, trusted exchanges of PDMP data and promote consistency among PDMPs.
- **NIEM:** NIEM is an XML information exchange standard which specifies the foundation and building blocks for interoperable information exchange by serving as a common XML vocabulary, integrated with established information exchange standards and processes, to support cross-domain information sharing and efficient information exchange between inter-related public and private service domains (e.g., law enforcement, public safety, healthcare, etc.). NIEM enables agencies to share information that crosses system, agency, and jurisdictional borders. NIEM improves decision-making, agility, and efficiency in satisfying business needs. NIEM supports interoperability and reuse, reducing costs.
- **NCPDP:** NCPDP is a not-for-profit, multi-stakeholder forum for developing and promoting industry standards and business solutions that improve patient safety and health outcomes, while also decreasing costs. NCPDP uses a consensus-building process to create national standards for real-time, electronic exchange of healthcare information. Their primary focus is on information exchange for prescribing, dispensing, monitoring, managing, and paying for medications and pharmacy services crucial to quality healthcare.
- **HL7/FHIR:** HL7 are a set of international standards used to transfer and share data between various healthcare providers. It supports clinical practice and the management, delivery, and evaluation of health services by providing a framework (and related standards) for the information exchange, system integration, data sharing, and retrieval

of electronic health information. HL7 helps bridge the gap between health IT applications and makes sharing healthcare data easier and more efficient when compared to older methods.

- **HTML5:** It supports the rendering of information received by the user into an understandable & readable format by displaying the data on a user interface.

To configure the SRS Outbound Sender Endpoint section, the State PDMP Administrator must enter the requested information into the active data fields that fall under this section. All URL Paths and Outbound URLs for each interface are auto populated. Should there be any questions or concerns, please contact the RxCheck technical team for further assistance.

The following Screenshot depicts the configuration process for the SRS Outbound Sender Endpoint section. For additional clarity, the ensuing table provides a definition of each data field present in the screenshot.



Heading	Data Field Name	Description
	Protocol	Protocols define a standardized set of rules for formatting and handling data during transmission. State PDMP Administrators must select one of the following options from the dropdown menu: • **HTTP (HyperText Transfer Protocol) –** A basic protocol used for transmitting text-based data between a client (e.g. browser) and a server. HTTP does not provide encryption, making it less secure for transmitting sensitive information. • **HTTPS (HyperText Transfer Protocol Secure) –** An enhanced version of HTTP that uses encryption and authentication mechanisms. HTTPS ensure secure communication be leveraging Secure Socket Layer (SSL) or Transport Layer Security (TLS), and is the recommended protocol for transmitting PDMP data within the RxCheck infrastructure.
	Domain	The domain name of the server on which the SRS is running. This field is <u>optional</u> – If no domain is specified the system will use the IP Address. E.g. New Jersey: NJ.gov
	Port Number	A port is a communication endpoint, and a port number is a logical number assigned to it. The port number indicates the dedicated port that will be used by the SRS software for communication purposes. Port numbers are used to direct incoming network traffic to the appropriate process or service on a server, ensuring that messages reach the correct application for handling.
	IP Address	An Internet Protocol (IP) Address is a unique numerical identifier assigned to each device that is connected to a network that uses the Internet Protocol for communication. The IP Address field is populated as “localhost” by default.

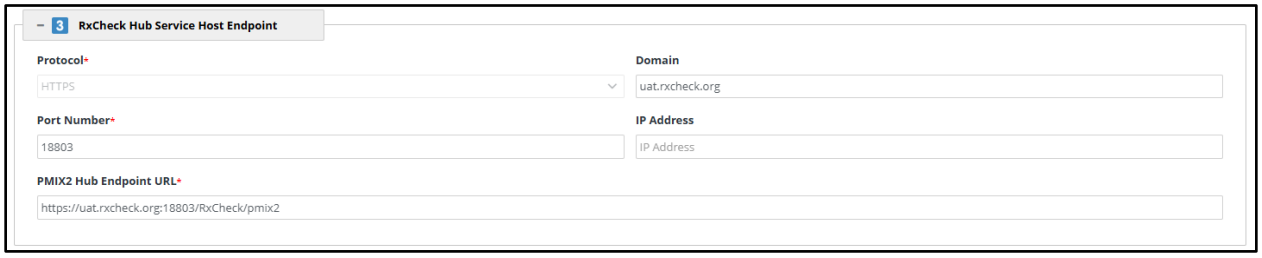
Heading	Data Field Name	Description
NIEM	**PMIX Outbound URL**	A fully qualified URL for the NIEM Service on Outbound SRS. ***This field is auto-populated.***
NCPDP-2017	**NCPDP-2017 Outbound URL**	A fully qualified URL for the NCPDP 2017 Service on Outbound SRS. ***This field is auto-populated.***
HL7 FHIR	**FHIR Outbound URL**	A fully qualified URL for the FHIR Service on Outbound SRS. ***This field is auto-populated.***
HTML	**HTML Outbound URL**	A fully qualified URL for the HTML Service on Outbound SRS. ***This field is auto-populated.***
Security Credentials: (HTTP Basic Authentication)	**Outbound Username**	A username to authenticate the SRS connection on the RxCheck network.
	Outbound Password	A password to authenticate the SRS connection on the RxCheck network.

7.3. RxCheck Hub Service Host Endpoint

The RxCheck Hub Service Host Endpoint section is a critical part of configuring the hub connection with the RxConsole application. The RxCheck Hub, a core component of the PMIX architecture, functions as a fully operational data-sharing system that allows states to securely and efficiently exchange Prescription Drug Monitoring Program (PDMP) data with other states and integration partners (e.g. Health Information Exchanges (HIE) and Electronic Health Records (EHR)).

All data fields in this section are auto-populated by the system, based on the information originally entered by the Super Administrator during site creation. State PDMP Administrators can review this information and should contact the RxCheck technical team if any discrepancies or concerns arise.

The screenshot below shows the configuration interface for this section. The accompanying table provides details descriptions for each data field presented.

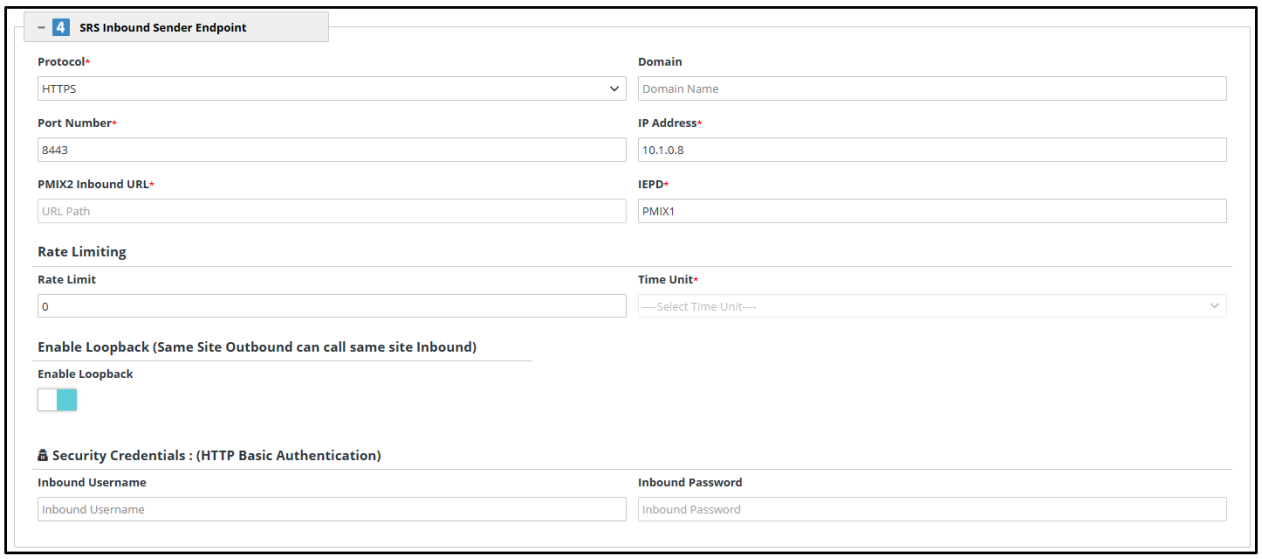


Data Field Name	Description
Protocol	This value cannot be changed and is set to “HTTPS”.
Domain	This value cannot be changed and is automatically set to the hub domain name.
Port Number	This value cannot be changed and is automatically set to the port on which the Hub is running.
IP Address	This value cannot be changed and is automatically set to the IP address for the Hub.
PMIX2 Hub Endpoint URL	***This field is auto-populated.*** It is a fully qualified URL for the PMIX2 NIEM4 service on the RxCheck Hub.

7.4. SRS Inbound Sender Endpoint

The SRS Inbound Sender Endpoint configuration enables the State PDMP system to receive incoming queries initiated by other states. To complete this configuration, the State PDMP Administrator must input the required information into the specified data fields within this section.

The screenshot below illustrates the configuration interface for the Inbound Sender Endpoint. For additional clarity, the following table provides detailed descriptions of each data field shown in the screenshot.



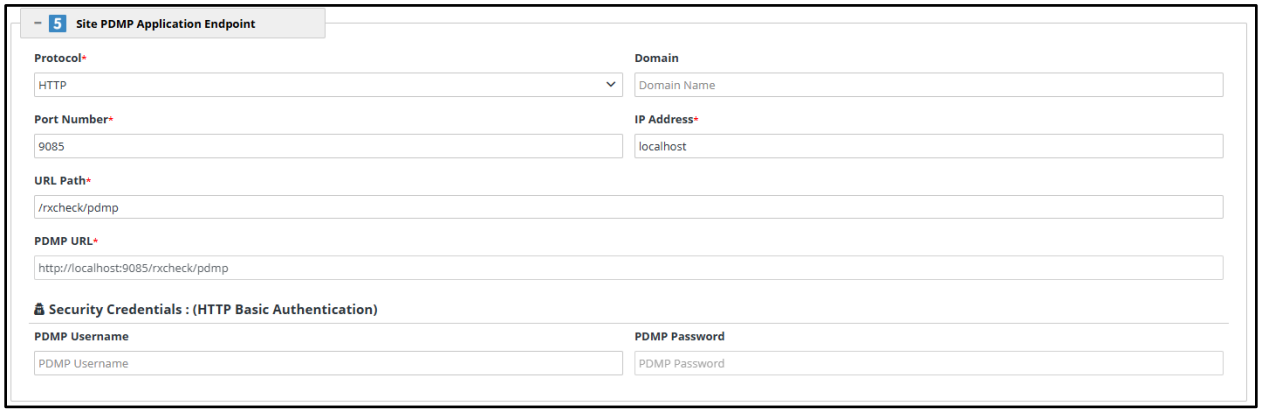
Heading	Data Field Name	Description
	Protocol	This value can be set to “HTTP” or “HTTPS”.
	Domain	The official website address of the PDMP’s Inbound Service instance. This field is <u>optional</u> – if the domain is not provided, the system will automatically take the IP address.
	Port Number	Port number where the Inbound Service is configured.
	IP Address	IP address where the Inbound SRS is hosted.
	PMIX2 Inbound URL	***This field is auto-populated*** based on the values selected/entered in the Protocol, Domain, IP address, and Port number fields. It is a fully qualified URL for PMIX2 NIEM4 Service on Inbound.
	IEPD	***This field is auto-populated*** based on IEPD option selected by Super Administrator at the time of PDMP Site creation. The value indicates the type of PDMP site. This indicates the PMIX version supported by PDMP.
Rate Limiting	**Rate Limit**	If a value is entered for this field, it indicates the number of Requests to the inbound with respect to the defined time unit.
Rate Limiting	**Time Unit**	Defines the unit for the value entered in the *Rate Limit* field. Can be set to Second, Minute, Hour, Day, or Month.

Heading	Data Field Name	Description
Enable Loopback (Same Site Outbound can call same site inbound)	**Enable Loopback**	This is a toggle button. When enabled (blue), it indicates that the users in the PDMP state can make Prescription Data requests to the same PDMP State. For example, if it is enabled for the PDMP State of NJ, it will indicate that NJ users can send the Prescription Data Requests to NJ. If the box is gray, it is disabled.
Security Credentials (HTTP Basic Authentication)	**Inbound Username**	A username to authenticate the SRS connection in the RxCheck network.
	Inbound Password	A password to authenticate the SRS connection in the RxCheck network.

7.5. Site PDMP Application Endpoint

This section defines the technical parameters of the state's PDMP application necessary for message routing and integration. To configure this section, the State PDMP Administrator must enter the required information into the designated data fields.

The screenshot below demonstrates the configuration interface for this section. For additional clarity, the accompanying table provides descriptions for each data field shown in the screenshot.



Heading	Data Field Name	Description
	Protocol	This value can be set to "HTTP" or "HTTPS".
	Domain	The website address of the PDMP state. This field is <u>optional</u> – if the domain is not provided, the system will automatically take the IP address.
	Port Number	Port number where the website is hosted.

Heading	Data Field Name	Description
	IP Address	IP address of the state PDMP server where the website is hosted.
	URL Path	This is the base URL or path for the PDMP Application endpoint for all the requests. The value for this field is based on the IEPD option selected by Super Administrator at the time of PDMP Site creation.
	PDMP URL	***This field is auto-populated*** based on the values selected/entered in Protocol, Domain/IP Address, Port Number.
Security Credentials (HTTP Basic Authentication)	**Inbound Username**	A username and is an optional parameter which enables basic authentication on PDMP Site.
	Inbound Password	A password and is an optional parameter which enables basic authentication on PDMP Site.

7.6. SRS Certificate

Each state is responsible for generating its own digital certificate using Microsoft PowerShell. Detailed instructions for this process are provided in the SRS Installation Guide for PDMP.

The certificate, created by the PDMP state implementing the SRS software, supports secure end-to-end message encryption. The SRS certificate uses a public key/private key infrastructure:

- The **public key** (contained in the certificate) is used to encrypt outgoing messages.
- The **private key** is used by the receiving system to decrypt the message.

Important: The certificate includes two components:

1. **Private Key—**Must be kept confidential and never shared, including within the RxCheck Network.
2. **Public Key—**Uploaded to the RxConsole and shared with other participating states in the RxCheck Network.

The State PDMP Administrator must input the required data into the fields provided under the SRS Certificate section.

The screenshot below illustrates the configuration interface for this section. For added clarity, the subsequent table provides descriptions for each data field shown in the screenshot.

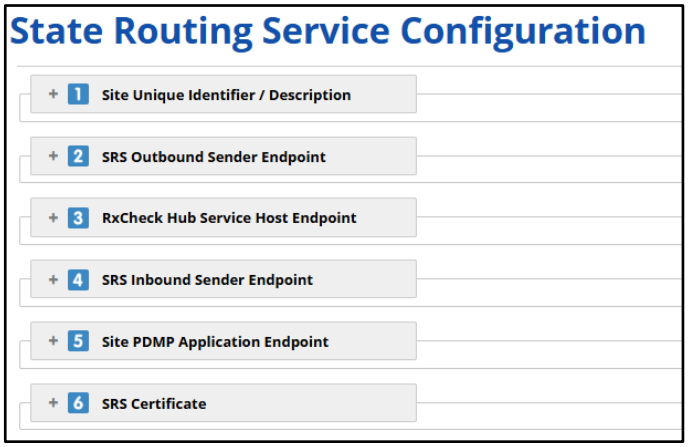
Data Field Name	Description
Private Key Subject	The key generated at the time of Site Certificate creation. The private key is in .pfx format. The Private key must be kept confidential by the PDMP State.
Public key (DER Format)	The key generated at the time of Site Certificate creation and is in .der format. The Public key is shared by the PDMP State with other PDMP States in the RxConsole Application.
Certificate Expiry Date	The date when the uploaded certificate expires.

7.7. Configure the SRS

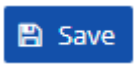
Once the previous sections have been populated on the State Routing Service Configuration page, the State PDMP Administrator can save the details and complete the configuration process.

1. Click on the *State Routing Service Configuration* button, located on the left-hand side of the screen.

2. Enter all required information. Mandatory fields are designated by a red asterisk (*) and need to be populated for the form to be saved successfully.
    a. You may need to click on the box for each step to expand that section and reveal the fields.



3. Click the *Save* button

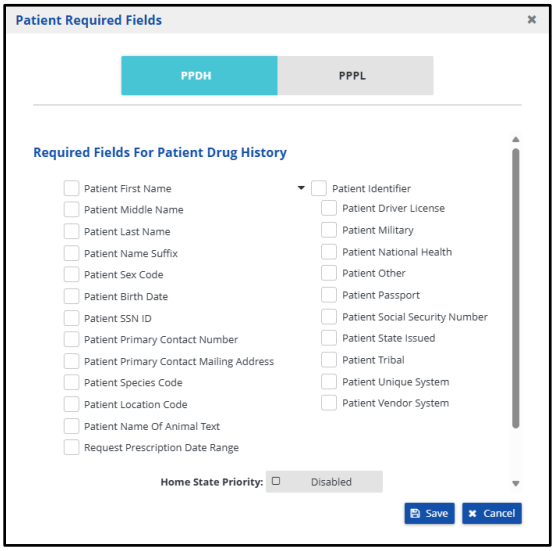


7.8. Configuring the required fields

Each State PDMP Administrator can configure the PMIX fields required in the request message to search for a patient in the PDMP system. The name-matching algorithm implemented within the PDMP system determines these required fields.

A PDMP administrator can configure these fields by navigating to the SRS Configuration page and clicking on the Patient Required Fields button.

Set the required fields for the patient prescription drug history (PPDH) and the patient prescription picklist (PPPL) queries.



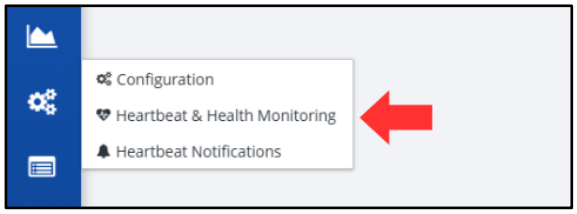
When processing an integration request involving a federated query, you can choose to enforce your state's data requirements by enabling the Home State Priority option. This will reject the entire request if it does not meet the required fields defined by your state.

7.9. Heartbeat and Health Monitoring

RxConsole includes the functionality to monitor the SRS when one is connected (See previous section titled *Configure the SRS* for steps on connecting the SRS). Monitoring is important to gain a better understanding of how the SRS and RxCheck are functioning and if there are any issues with integrations. The subsections below explain the health monitoring available to RxConsole users.

7.9.1 Current Site Monitoring

1. Click on the *State Routing Service* button, followed by the *Heartbeat & Health Monitoring* option, located on the left-hand side of the screen.

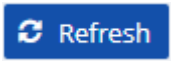


2. By default, you will be at the current site *SRS: Heartbeat and Health Monitoring* screen.

3. This screen includes various graphs to show the current status of the SRS.

   Note: The table at the end of this section includes additional information regarding what is monitored in each graph.

4. A user can click the *Refresh* button to get the most up to date information regarding their SRS.



5. A user can click the *Show last 10 Pings* button to view a table of the last 10 pings to the SRS.

Note: The headers in the table are described in the following table.

Header	Description
DeviceID	An identification code that references the device that pinged the SRS.
Host	A reference code to identify the RxConsole state and version that pinged the SRS.
InstanceID	Identification of the instance of the SRS that was pinged.
IP#	The IP address of the instance of the SRS that was pinged.
Site Code	The two letter code that references the state.
Time Stamp	The date and time the ping occurred.

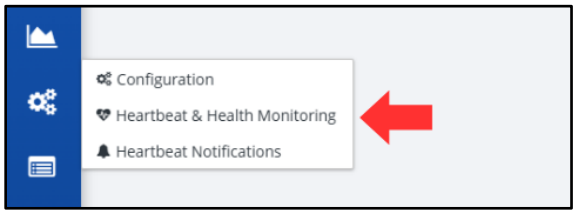
Graph Title	X-Axis	Y-Axis	Description
Status over a period of time with Timeline Bar	Time	Status—Up/Down	The status of the SRS over a period of time.
Instance Status	Time	Status—Up/Down	The status of the SRS over a period of time, allows you to use the dropdown to switch the instance.
JVM Threads	Time	Number of JVM Threads	Displays the number of active Java Virtual Machine (JVM) threads at regular time intervals. Rising lines may indicate increased load or usage and falling lines may suggest stable or reduced activity.

Graph Title	X-Axis	Y-Axis	Description
Garbage Collectors	Time	Time spent collecting and releasing the memory	Indicates how much time garbage collection took. Helps to identify memory issues which can impact application responsiveness.
CPU	Time	Percent usage	The amount of processing power used over time.
JVM Memory	Time	Size of JVM memory	Helps to detect trends such as memory growth, potential memory leaks, or inefficient memory usage patterns.
Disk Space Used	Time	Size of disk space	Helps identify storage trends, which may signal the need for a cleanup or capacity planning.

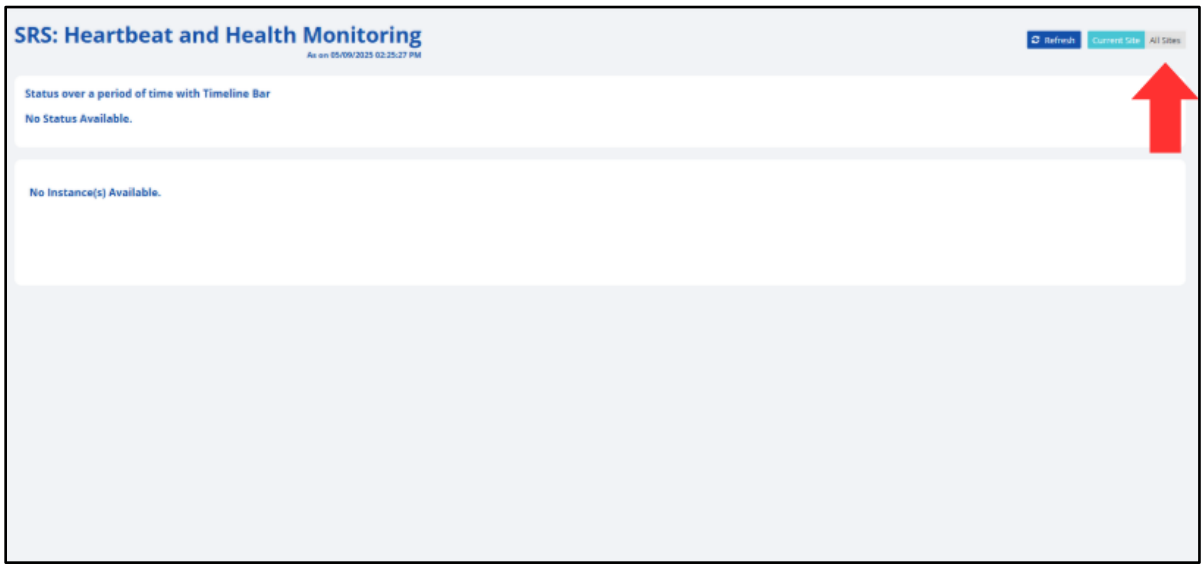
7.9.2. All Sites Monitoring

To navigate to *All Sites* monitoring, follow the steps below.

1. Click on the *State Routing Service* button, followed by the *Heartbeat & Health Monitoring* option, located on the left-hand side of the screen.



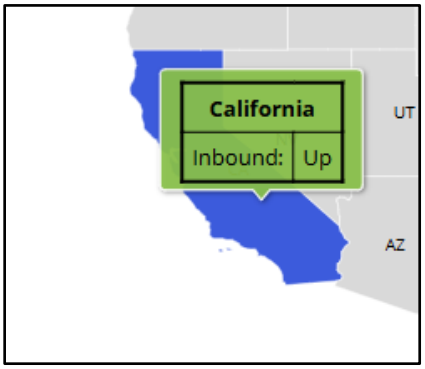
2. Click on the *All Sites* button in the top right corner of the screen.



3. The next screen is the *SRS: Heartbeat and Health Monitoring* screen and includes a United States Map.

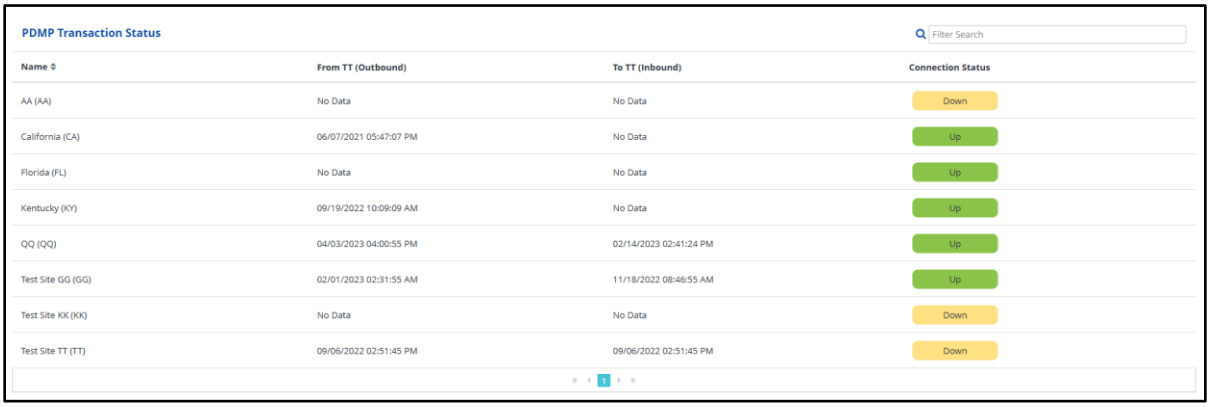
4. The map allows you to hover your cursor over a state and get the current status of their SRS server.

   Note: The states are color coordinated based on their SRS status. Please see the following table to better understand the colors.



5. Scrolling down on this screen, you are able to see a list of the States and their connection status in a table. The table also allows you to see the most recent query to or from a state.

   Note: The following table includes a description of each of the table headers.



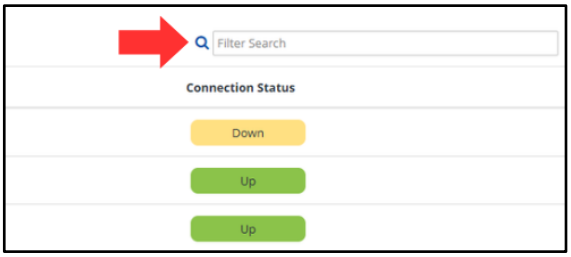
PDMP Transaction Status

Name	From TT (Outbound)	To TT (Inbound)	Connection Status
AA (AA)	No Data	No Data	Down
California (CA)	06/07/2021 05:47:07 PM	No Data	Up
Florida (FL)	No Data	No Data	Up
Kentucky (KY)	09/19/2022 10:09:09 AM	No Data	Up
QQ (QQ)	04/03/2023 04:00:55 PM	02/14/2023 02:41:24 PM	Up
Test Site GG (GG)	02/01/2023 02:31:55 AM	11/18/2022 08:46:55 AM	Up
Test Site KK (KK)	No Data	No Data	Down
Test Site TT (TT)	09/06/2022 02:51:45 PM	09/06/2022 02:51:45 PM	Down

6. You can search for a specific site by:
   a. Finding the state on the list using the page buttons under the table, or
   b. Searching for the state in the search box above the table.

a.

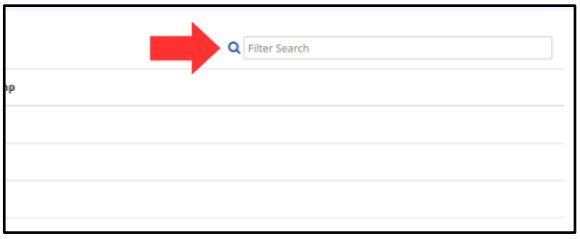
b.



7. Scrolling down further, the last table displays a list of the connected healthcare entities and the last time a query was received from them. A healthcare entity can be found by:
   a. Using the page buttons on the bottom of the table and looking for the entity, or
   b. Search for the site in the search bar above the table.

c.

d.



Status	Color Code	Color
Up	Green	
Down	Yellow	
N/A	Gray	
Currently Hovering	Orange	

PDMP Transaction Status Table

Heading	Description
Name	Name and 2 letter abbreviation for the state.
From [State Code] (Outbound)	The date and time of the last query from your state to listed state.
To [State Code] (Inbound)	The date and time of the last query from this state to the users state.
Connection Status	The current status of that states SRS.

HCE Transaction Status to TT (Inbound)

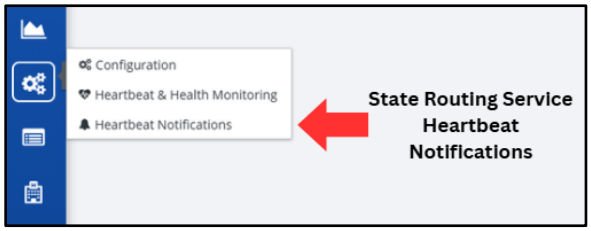
Heading	Description
Name	The HCE code to identify the appropriate healthcare entity.
Last Transaction Timestamp	The date and time of the last query from the healthcare entity to your state PDMP.

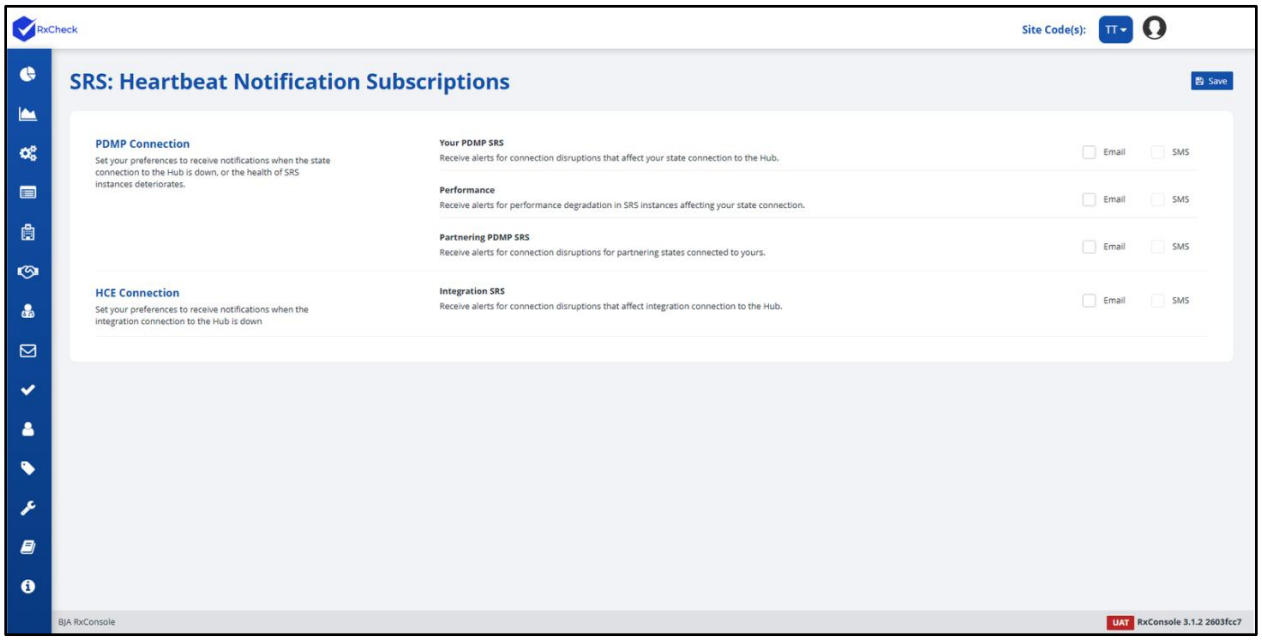
7.10. Heartbeat notifications

Using the Heartbeat Notifications feature, the PDMP Administrator can subscribe to receive email notifications and text messages about the PDMP and HCE connections.

To navigate to the Heartbeat notifications, follow the instructions below.

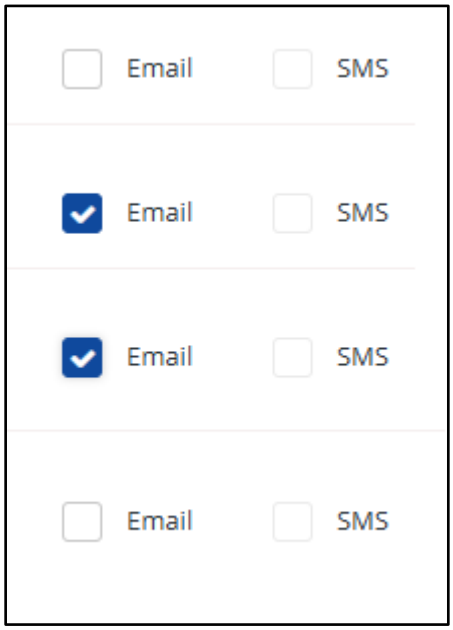
1. Click on the *State Routing Service* button, followed by the *Heartbeat Notifications* option, located on the left-hand side of the screen.



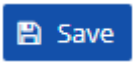


2. Select the desired boxes to subscribe to that notification.
   a. If the *Email* option is checked, the user will receive emails to the mailbox associated with their RxConsole application login.
   b. If the *SMS* option is checked, the user will receive text messages on the mobile phone number specified in their RxConsole application profile.

   Note: You will need to email the RxCheck admin to add a phone number to enable the SMS notifications option.



3. After making any changes, a user will want to press the *Save* button to process any changes made to notifications.



The table below explains the different subscription options that a PDMP administrator can subscribe to.

Heading	Subscription Option	Description
PDMP Connection	**Your PDMP SRS**	Receive alerts for connection disruptions that affect your state connection to the Hub.
	Performance	Receive alerts for performance degradation in SRS instances affecting your state connection.
	Partnering PDMP SRS	Receive alerts for connection disruptions for partnering states connected to yours.
HCE Connection	**Integration SRS**	Receive alerts for connection disruptions that affect integration connection to the Hub.

Note: Notifications are not immediate. A subscribed user will receive an email or SMS notification approximately 15 minutes after the first missed heartbeat is detected.

8. Hub Audit Logs

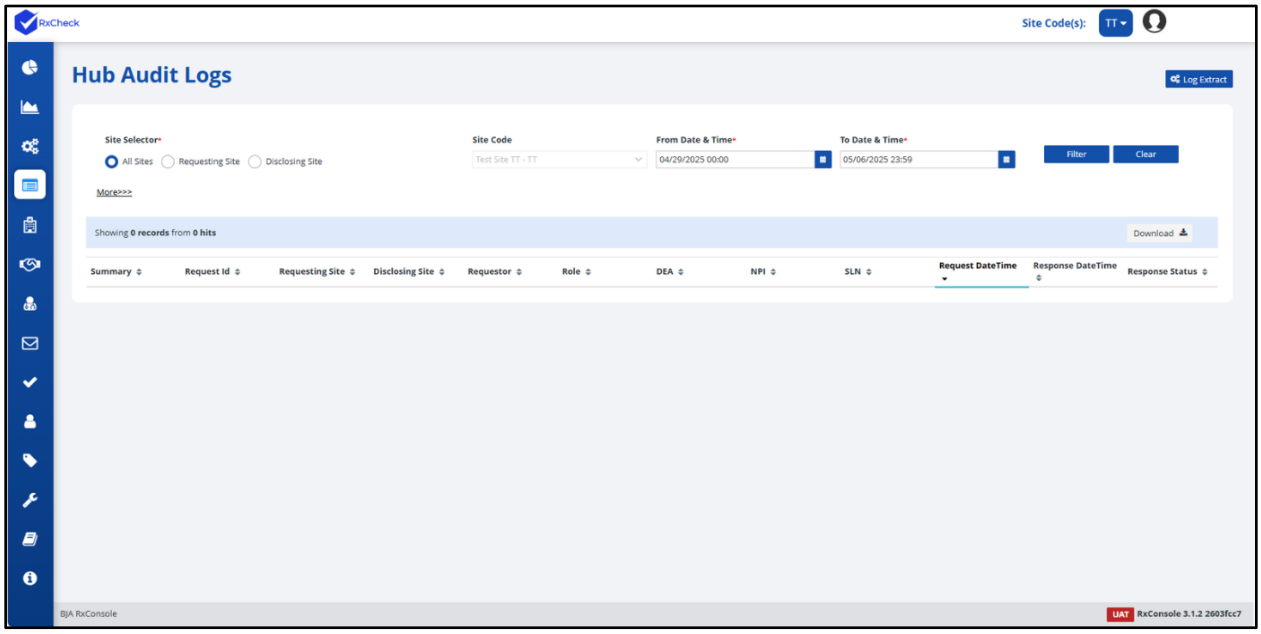
The Hub Audit Log captures detailed records of all incoming and outgoing transactions processed through the RxCheck Hub. This feature provides State PDMP Administrators with visibility into:

- The number of requests received by their state,
- The number of requests sent to other states, and
- The status of each transaction (e.g., Successful, Access Denied, Deferred, Failed due to Connection Error, etc.)

An Audit ID is automatically generated for each transaction that reaches the RxCheck Hub. These records are summarized and displayed in the Hub Audit Log section of the RxConsole application.

By clicking on an Audit ID, administrators can view a detailed summary of the associated transaction, including both request and response details involving the PDMP state. The Hub Audit Logs are also a valuable tool for diagnosing failed transactions and identifying the root cause of communication issues.

The following subsection provides step-by-step instructions for viewing the Hub Audit Logs within the RxConsole interface. Each step is accompanied by a screenshot to assist with navigation and understanding.



8.1. Read the hub audit logs

The following screenshot displays two hub audit log entries.

Showing **1000 records** from **2537 hits**

Audit Id	Request Id	Requesting Site	Disclosing Site	Requestor	Role	DEA	NPI	Request Datetime	Response Datetime	Response Status
b81027c2-bccd-46e9-9800-8fc8fd64b27f	20200211A	TT_PMX	TT	BLOCK_TEST_1	PhysiciansX			09/28/2020 09:42:45 AM	09/28/2020 09:42:45 AM	Access Denied
d01a69b6-dd09-4393-b5ee-55e6930111aa	20200211A	TT_PMX	TT	BLOCK_TEST_1	Physicians			09/28/2020 09:41:30 AM	09/28/2020 09:41:30 AM	Connection Error

Clicking on the blue hyperlink text will display additional information about its column.

For example, clicking on one of the Audit ID values will display the following Log Summary pop-up page. The Log Summary contains additional information about the respective transaction and may add further insight (in the “Message” section) as to why a transaction was not successful.

Log Summary

Message Id	uuid:1139949a-6e9a-4176-b6f0-500d5b4dfb0b		
Audit Id	d01a69b6-dd09-4393-b5ee-55e6930111aa		
Request Id	20200211A	**Request Status**	Connection Error
Requesting Site	TT_PMX	**Disclosing Site**	TT
Requestor	BLOCK_TEST_1	**Requestor Role**	Physicians
DEA Number		**NPI Number**	
Request Time	09/28/2020 09:41:30 AM	**Response Time**	09/28/2020 09:41:30 AM

Error Log

Http Status	500
Reason	EXCEPTION
Detail	Error : Server returned HTTP response code: 500 for URL: https://localhost:12083/rxinbound/service/inbound?wsdl
Message	`<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"><soap:Header> <wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd" soap:mustUnderstand="true"><wsu:Timestamp wsu:Id="TS-18f246c1-31f2-4ccd-8507-d3950dd58740"><wsu:Created>2020-09-28T13:41:30.948Z</wsu:Created><wsu:Expires>2020-09-28T13:46:30.948Z</wsu:Expires> </wsu:Timestamp><xenc:EncryptedKey xmlns:xenc="http://www.w3.org/2001/04/xmlenc#" Id="EK-5f0a81a5-7c55-43ff-aac9-0c983350f98d"><xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><wsse:SecurityTokenReference> <wsse:KeyIdentifier EncodingType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary" ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-`

The following table details the role of each column title displayed in the Hub Audit Log.

Title	Description
Summary	Provides details about the transaction and any errors.
Request ID	The ID provided in a request transaction that is made to obtain prescription data of an individual patient.
Requesting Site	The state code of the State that initiated the data request.
Disclosing Site	The state code of the State to which the data request is being sent to.
Requestor	The name of the healthcare professional who submitted the request.
Role	The role of the healthcare professional who submitted the request.
DEA	The Drug Enforcement Administration number of the healthcare professional who submitted the request.
NPI	The National Provider Identification number of the healthcare professional who submitted the request.
SLN	The State License number of the healthcare professional who submitted the request.
Request DateTime	The date and time the request was initiated.
Response DateTime	The date and time the response was sent.
Response Status	The status of the transaction.

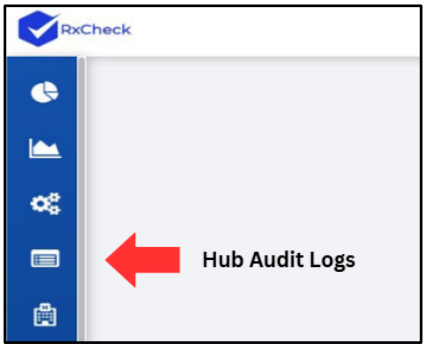
The following table describes what each of the available *Request Status* options translates to.

Status	Description
Provided	A query was received, and a result was returned without issue.
Deferred	*Internal only- for debugging purposes
Not Found	A query was received, but a patient match was not found. In some cases, Not Found will also be the response when too many patients were found and a guaranteed match could not be established.
Disallowed	*Internal only- for debugging purposes
Invalid Document	*Internal only- for debugging purposes
Invalid Response	*Internal only- for debugging purposes
No Route Found	There is no message route found to forward the request to a PDMP.
Access Denied	A query was received, but the disclosing state denied the request (often due to not allowing the requestor's role access to data).
Outbound Certificate Expired	The sending state's certificate has expired.

Status	Description
Inbound Certificate Expired	The receiving state's certificate has expired.
Invalid Site Code	An invalid site code was sent in the message.
Max Limit Reached	When the number of messages reaches the threshold that the PDMP Administrator sets in the hub.
Timeout	The request timed out while waiting for the response.
Connection Error	There was an error connecting the requesting entity to the SRS.
Validation Failed	A query was received, but the requestor did not pass validation rules set up in the RxConsole for the state.
Version Mismatch	*Internal only- for debugging purposes
Error	*Internal only- for debugging purposes
Connection Reset	There is a TCP/IP connection reset that occurred.
Service Not Available	Displays when any of the internal services are not available to process the message.
Site not found	An invalid site code was sent in the message.

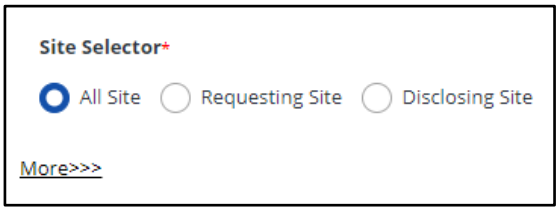
8.2. Filter the hub audit logs

1. Click on the *Hub Audit Logs* button, located on the left-hand side of the screen.



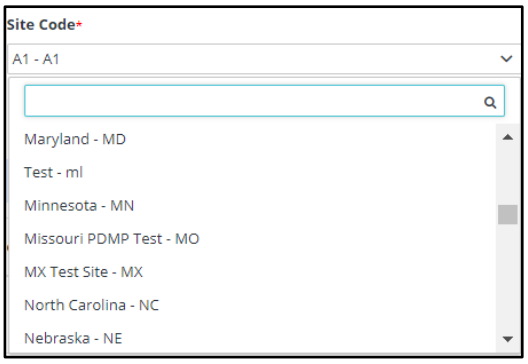
2. Select the appropriate *Site Selector* option:
   - **All Site-** Lists all incoming and outgoing requests to/from your state.
   - **Requesting Site-** A state that sent a request to your state.
   - **Disclosing Site-** A state that received a request from your state.

   Note: This is a required field and is set to *All Site* by default.



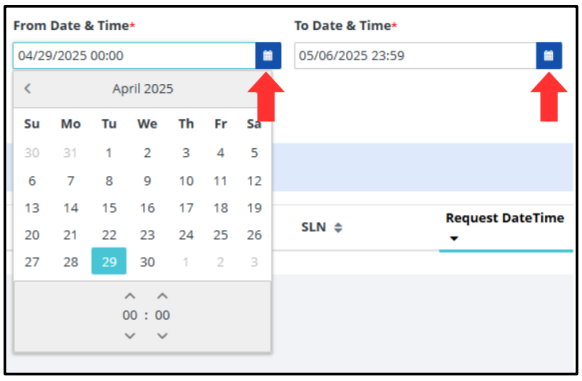
3. Select the *Site Code* by clicking the down arrow and then:
   a. Scrolling through the dropdown options and checking the box, or
   b. Typing in the search bar to filter results.

   Note: This filter is only active when *Disclosing Site* or *Requesting Site* is selected in the *Site Selector* in step 2 above. This field is required.



4. Select the date and time range to filter the audit log:
   a. From DateTime – Start date and time
   b. To DateTime – End date and time

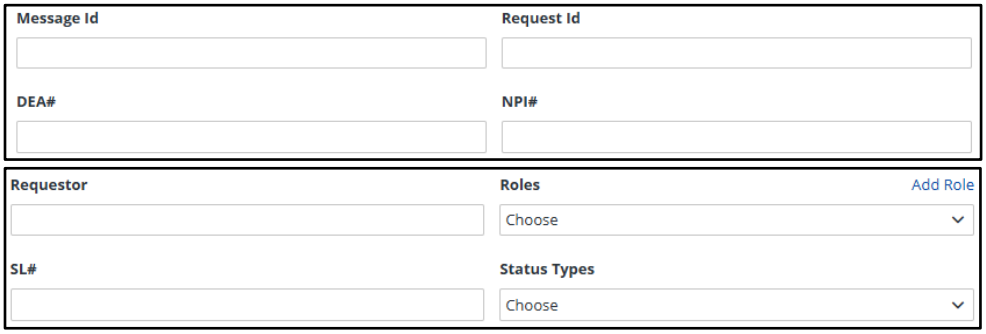
   Click the blue calendar icon to choose a date. Use the left/right arrows to switch months. Adjust the time using the up/down arrows below the calendar (24-hour format: HH:MM).



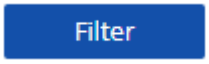
5. Clicking on the *More>>>* link located below the *Site Selector* filter will provide additional filtering options.

6. The following additional filter options are available:
   a. Message ID
   b. Request ID
   c. Requestor
   d. Roles
   e. DEA#
   f. NPI#
   g. SL#
   h. Status Types

Enter an appropriate value into your desired filter option field. An explanation of each field is listed in a table following these steps.



7. Click on the *Filter* button to apply the selected Hub audit log criteria.



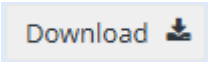
8.3. Download the hub audit logs

The RxConsole application allows PDMP Administrators to download a copy of their audit logs. When downloaded, the audit logs are packaged as a zipped file.

After downloading the zipped file, users can extract its contents and save them to a preferred location on their computer. The extracted file is in Comma-Separated Values (.csv) format and can be opened using Microsoft Excel or any other software that supports CSV files.

1. Perform any filtering desired using the steps in the previous section.

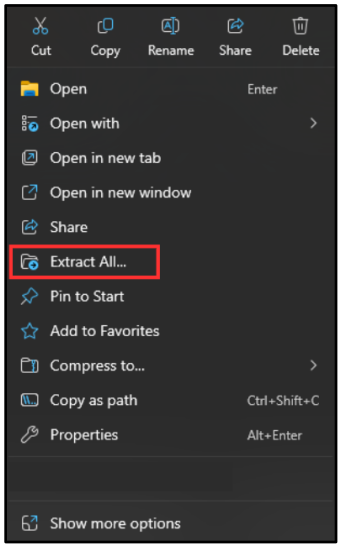
2. Click on the download button on the right-hand side of the screen.



3. The hub audit logs will be saved to your computer in a zipped folder.

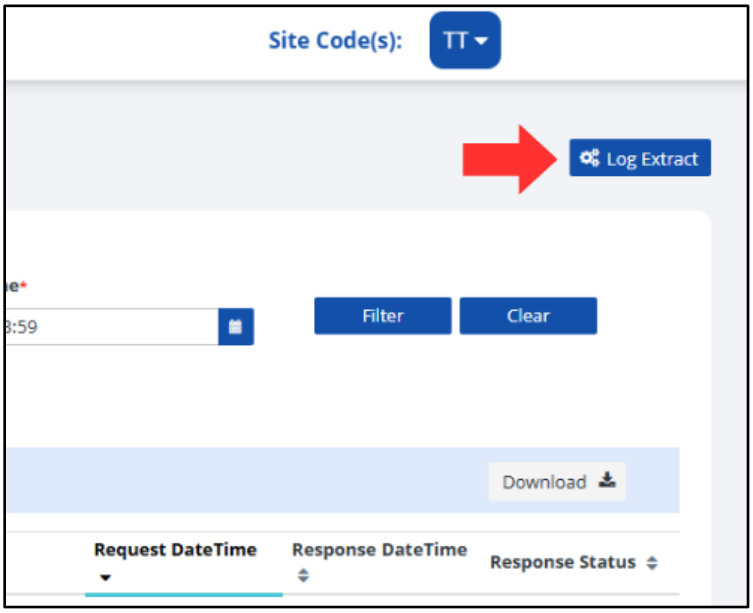
4. Right-click on the zipped folder to view options

5. Select the “Extract All…” option.

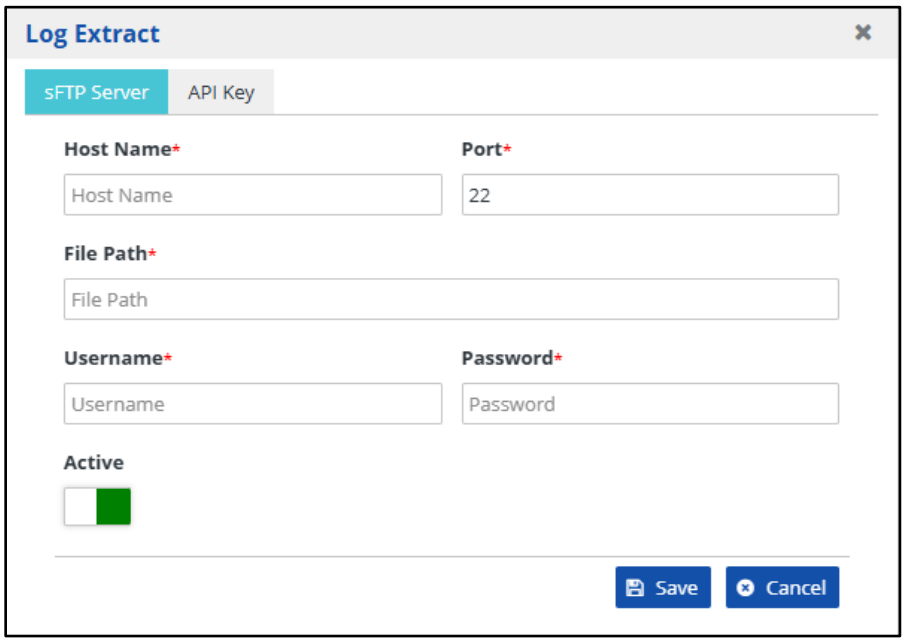


8.4. Exporting the logs to an sFTP server

RxConsole enables PDMP Administrators to export RxCheck Hub audit logs to their state’s sFTP server by providing the required sFTP configuration—hostname, port, username, and password—via the “Log Extract” section on the Hub Audit Logs page.



After clicking the *Log Extract* button, you will see the following window.



The following table includes a description of each of the fields available.

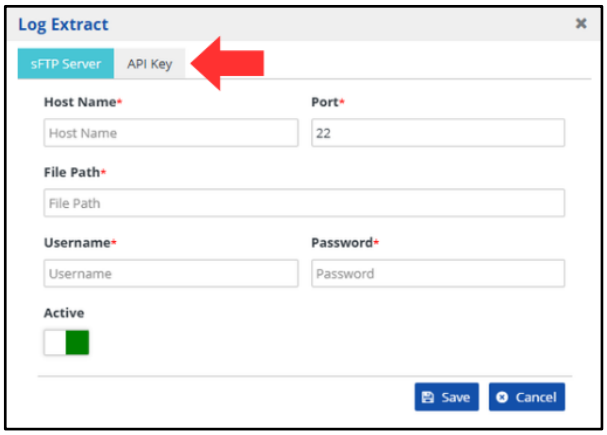
Field	Description
Host Name	The domain name or IP address of the remote SFTP server. Example: sftp.example.com or 192.168.1.100.
Port	The port number used for the sFTP connection. The default is “22”, but it can be configured to other values by the server administrator.
File Path	The directory path on the remote server where files will be uploaded to or downloaded from. Example: /home/sftp,_user/uploads, or /data/incoming.
Username	The login name used to authenticate the user with the SFTP server. It is typically assigned by the server administrator.
Password	The secret key or password corresponding to the username for authentication. This can be omitted if key-based authentication is used.
Active	Allows a user to enable and disable the log extract function. When the box is green, it is enabled. When red, the functionality is disabled.

After the sFTP configuration is saved, the system will activate the *Export Logs (sFTP)* button for the PDMP administrator. To initiate the log export, click this button. The system will process the request and send an email notification once the export is complete.

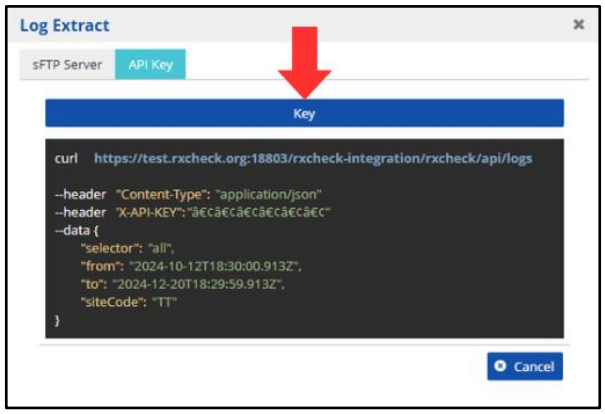
8.5. Using an API to download the logs

RxConsole also allows a PDMP Administrator to enable an API endpoint to download audit logs from the RxCheck Hub. To access this API, an API key is required.

1. From the log extract window, select the *API Key* tab.



2. Press the *Key* button to generate an API key.



3. To copy the API Key, press the *copy* button.

4. To create a new unique API key, press the *ReGenerateAPIKey*.

5. To remove your API, press the *Delete* key.

Note: The system generates a sample API request to be used as a reference for developing a module to download Hub audit logs.

9. Healthcare Entities

A Healthcare Entity (HCE) refers to any licensed healthcare provider or organization that is authorized by its respective state to deliver professional healthcare services. This includes:

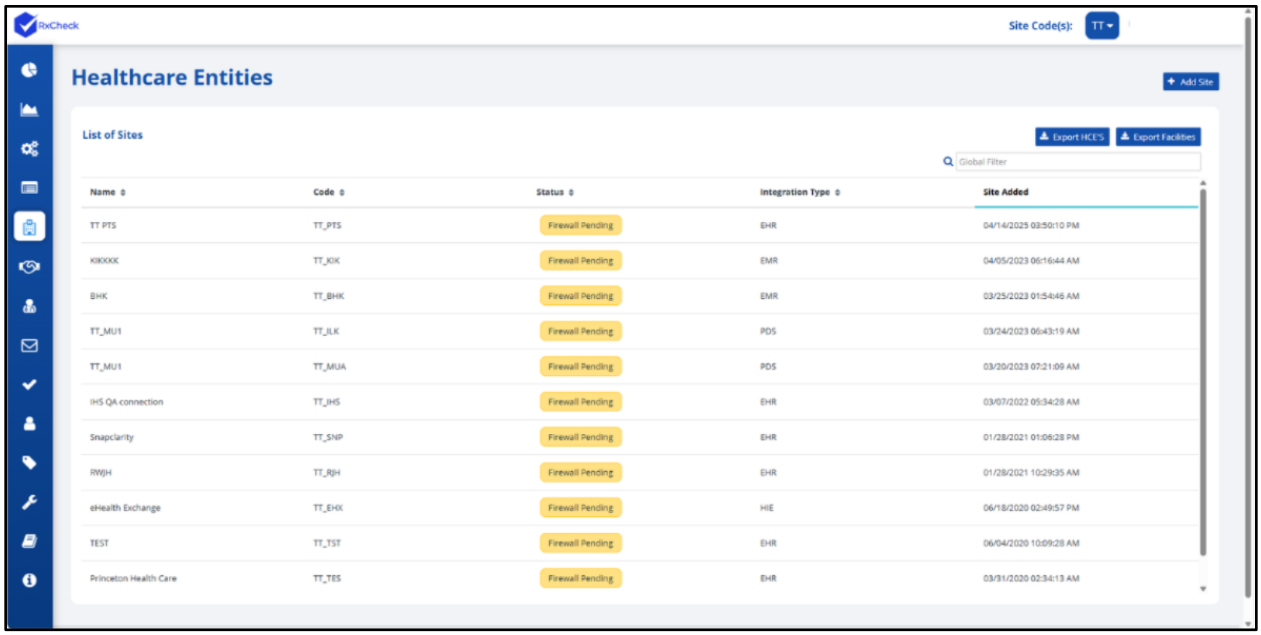
- Individual providers licensed to practice healthcare,
- Healthcare organizations employing licensed professionals, and
- eHealth Exchange organizations recognized by the state for providing licensed healthcare services.

A healthcare entity can only submit patient data requests and receive responses through RxCheck after it has been officially onboarded into the state's RxCheck system.

When a new healthcare entity expresses interest in participating in RxCheck, the State PDMP Administrator can initiate onboarding by creating a new entity site. This is done by clicking the *+ Add Site* button located in the top right corner of the Healthcare Entities page.

Administrators can also view and manage existing healthcare entity records associated with their state. The full list of onboarded entities can be accessed by selecting the *Healthcare Entities* icon from the left-hand navigation panel.

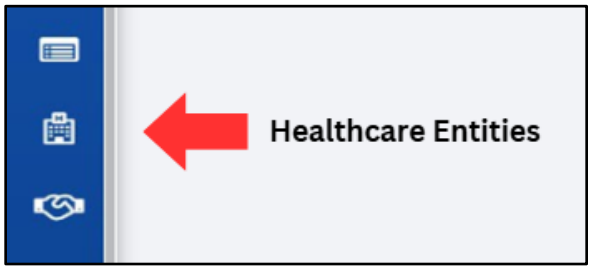
The screenshot below displays an example list of onboarded healthcare entities within a state's PDMP system. The accompanying table provides definitions for each column heading show in the interface.



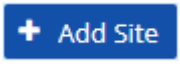
Heading	Description
Name	The name of the healthcare entity (HCE).
Code	A six-character code that follows the following format: • Two letters to represent the state code. • An underscore (_). • Three letters to represent a HCE site.
Status	Indicates the current status of an HCE. • Active- the HCE is currently active. • Inactive- the HCE is currently inactive. • Firewall Pending- the HCE is currently active but was recently set up.
Integration Type	Refers to the site type value that was selected when the HCE was created. This value will be displayed as one of the following: • EHR – Electronic Health Records • EMR – Electronic Medical Records • HIE – Health Information Exchange • PDS – Pharmacy Dispensing System
Site Added	Date and time when the HCE site was created.

9.1. Add a new healthcare entity site

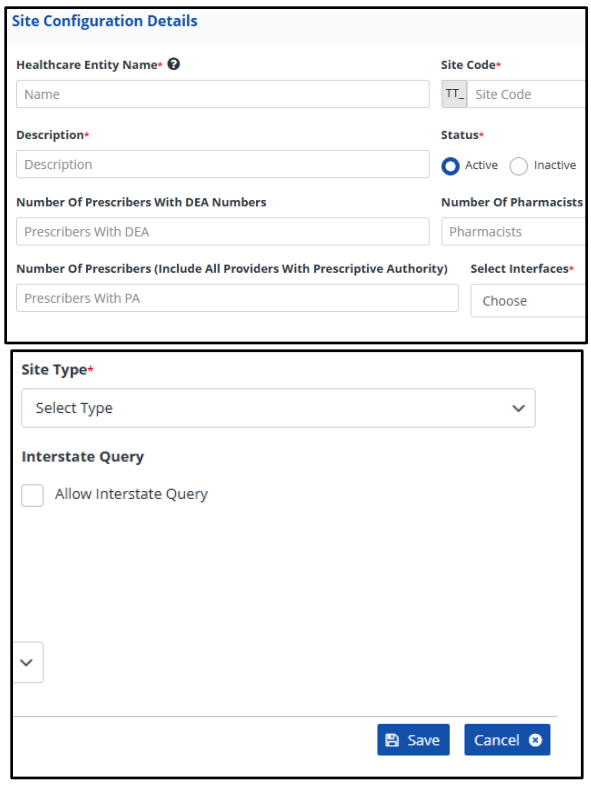
1. Click on the *Healthcare Entities* button, located on the left-hand side of the screen.



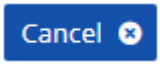
2. Click on the *+ Add Site* button.



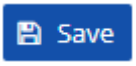
3. Populate the Site Configuration Details for the new healthcare entity.
   Refer to the "Breakdown of Healthcare entity site details" section below for field-specific guidance.



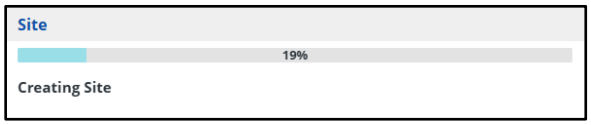
4. To exit without saving, click the *Cancel* button.



5. To save the populated site information, press the *Save* button.

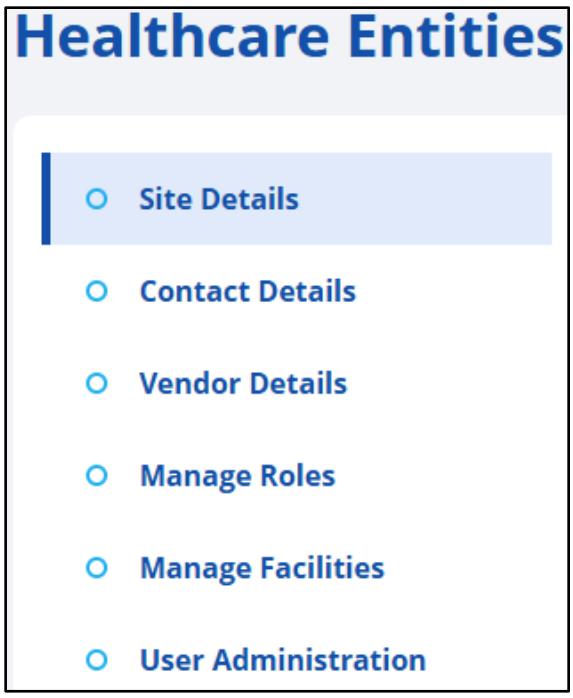


6. Wait patiently as your site is being created.



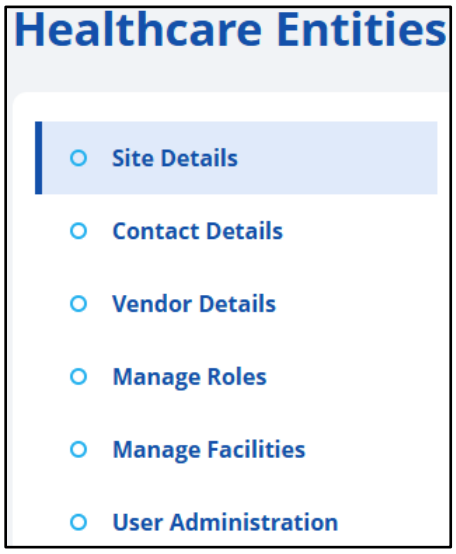
7. Populate additional details as requested in the corresponding data fields for each section.

   Refer to the "Breakdown of Healthcare entity site details" section below for field-specific guidance.



9.2. Breakdown of Healthcare entity site details

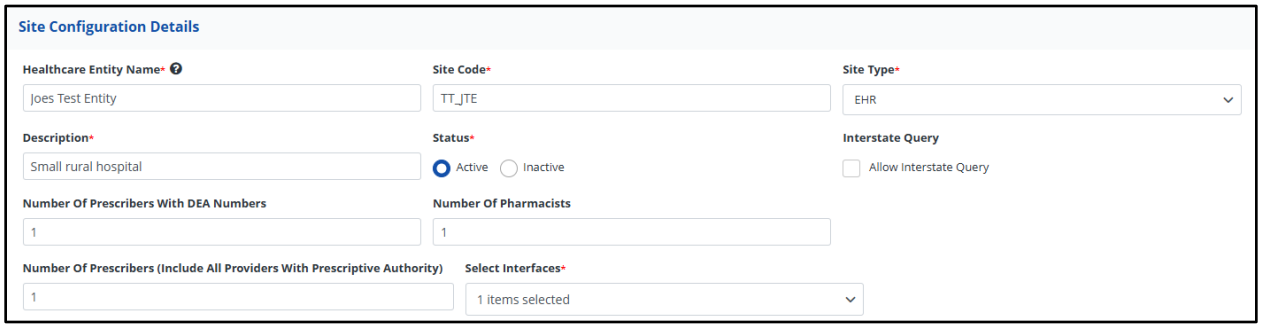
Once a healthcare entity record is created, the user will be able to add, view and manage the following details by clicking on the respective menu options.



The following subsections provide a detailed breakdown of each data field, as displayed on each menu option/section of a healthcare entity's record.

9.2.1. Site Details

This section displays information related to this specific HCE.



Heading	Description
Healthcare Entity Name	The name of the Healthcare Entity.

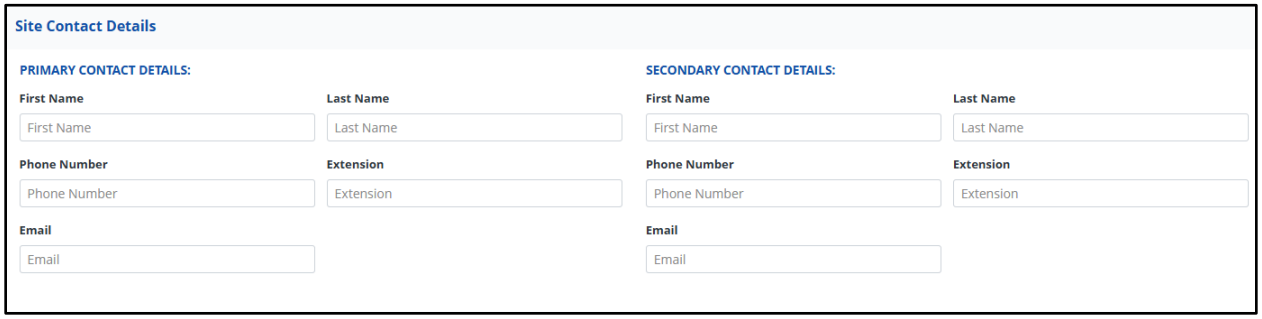
Site Code	A six-character code that follows the following format:
	• Two letters to represent the state code. This is auto-populated.
	• An underscore (_).
	• Three letters to represent a HCE site. These are entered by the PDMP administrator.
	  ○ When deciding on the three letters to represent a HCE, think of the initials for the company. Planning is often beneficial to avoid creating abbreviations that lead to confusion. One site code can cover multiple individual facilities within a state.
	  ○ Example: Walmart may be **WLT** or **WAL**, where Walgreens may be **WGN** or **WAL**.

Site Type	Refers to the site type. This value can be set as one of the following: • EHR – Electronic Health Records • EMR – Electronic Medical Records • HIE – Health Information Exchange • PDS – Pharmacy Dispensing System
Description	A simple description of the HCE site.
Status	Status that indicates if a site is *Active* or *Inactive*.
Interstate Query	When checked, the HCE will be able to send interstate data requests.
Number of Prescribers with DEA numbers	A count of prescribers with DEA numbers at that HCE.
Number of Pharmacists	A count of pharmacists at that HCE.

Heading	Description
Number of Prescribers (Include All Providers With Prescriptive Authority)	A count of all prescribers at that HCE.
Select Interfaces	The type of connection the HCE is using to connect to RxCheck or third-party integrator. The following options are available: • NCPDP2017 • HTML • FHIR3 • FHIR4 • PMIX2 • JSON

9.2.2. Contact Details

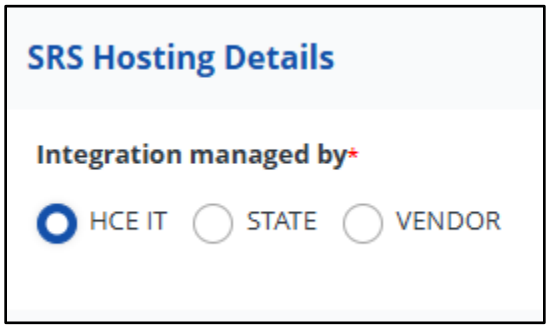
This section contains the primary and secondary contact information for individuals to contact for further inquiries related to this specific HCE.

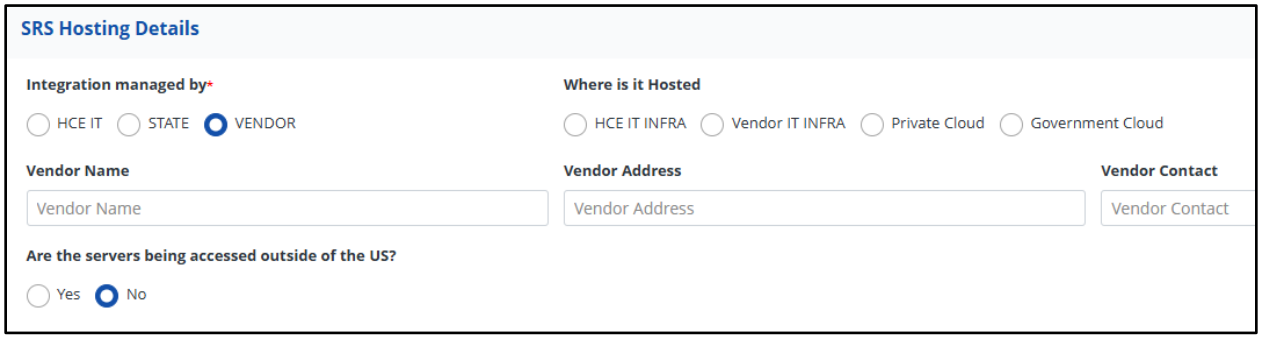


Heading	Description
First Name	Individual contact person's first name.
Last Name	Individual contact person's last name.
Phone Number	Individual contact person's phone number.
Extension	Individual contact person's phone number extension, if any.
Email Address	Individual contact person's email address.

9.2.3. Vendor Details

This section contains the SRS hosting details and indicates if the healthcare entity's integration is managed by the HCE IT team, the state, or by a vendor.





Heading	Description
HCE IT	This option indicates that the IT team of the HCE oversees the SRS hosting and managing responsibilities.
State	This option indicates that the IT team of the state oversees the SRS hosting and managing responsibilities.
Vendor	This option indicates that a third-party vendor (not the HCE) oversees the SRS hosting and managing responsibilities.

Note: If the *Vendor* option is chosen, additional fields need to be populated.

Heading	Description
Where is it Hosted	Refers to where the vendor hosts the SRS server for the HCE. The following options can be selected. • HCE IT INFRA – Hosted by the healthcare entity's infrastructure. • Vendor IT INFRA – Hosted by the vendors infrastructure. • Private Cloud – Hosted on a private cloud, accessible by only the HCE and/or vendor. • Government Cloud – Hosted on a government cloud, accessed by individuals outside the HCE or state PDMP team.
Vendor Name	The name of the vendor hosting the SRS.

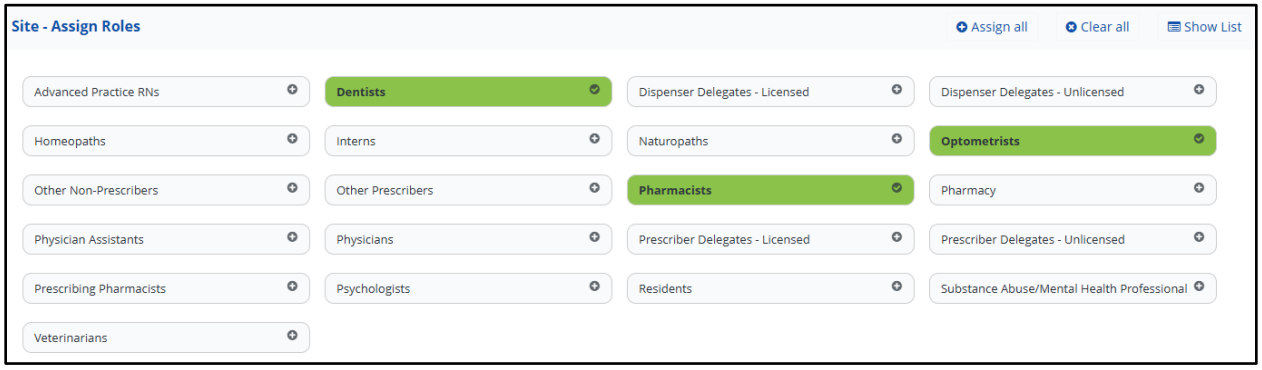
Heading	Description
Vendor Address	The address of the vendor hosting the SRS.
Vendor Contact	The name of the contact responsible for managing the SRS.
Are the servers being accessed outside the US?	A *Yes* or *No* question that asks if the SRS will be accessed for any reason outside the United States of America.

9.2.4. Manage Roles

This section enables the State PDMP Administrator to assign roles that authorize specific users within a healthcare entity to submit prescription data requests. Roles are assigned by selecting the appropriate tags associated with the healthcare entity.

Each tag corresponds to a recognized healthcare professional role or the type of services provided by the entity. These role assignments determine the level of access and functionality available to the entity within the RxCheck system.

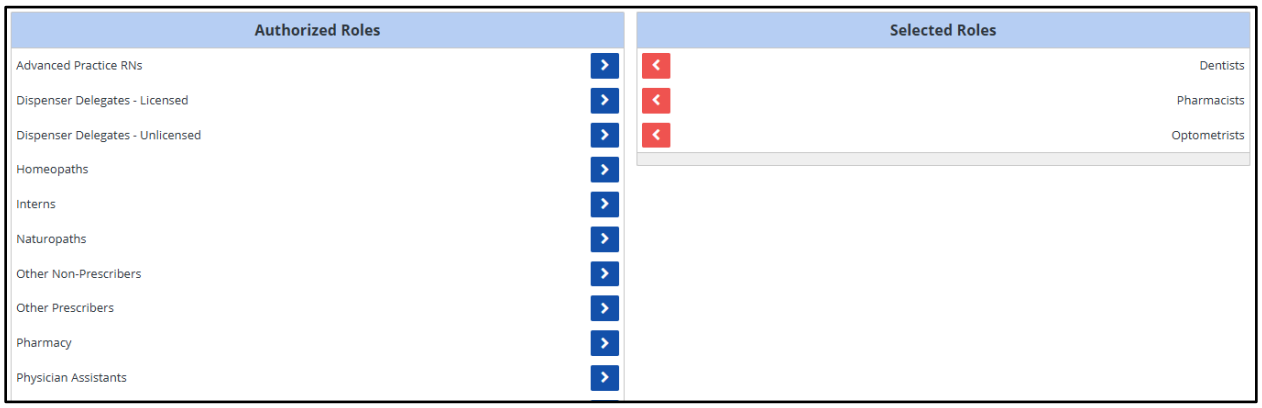
All available roles are displayed by default as shown below. Clicking on a role will change the role to green. A green highlighted role is active or "Selected" and allows that role to initiate a query, while an off-white color indicates that the role is "Authorized" but inactive and cannot initiate a query.



Button Name	Button Image	Functionality
Assign All	Assign all	Automatically selects all displayed roles.
Clear All	Clear all	Automatically deselects all displayed roles.
Show List	Show List	Will display all available roles in two separate lists, an *Authorized Roles* list and a *Selected Roles* list.
Hide List	Hide List	Will display all available roles as tags (default). **Note:** This option is only available when the roles are displayed as two separate lists.

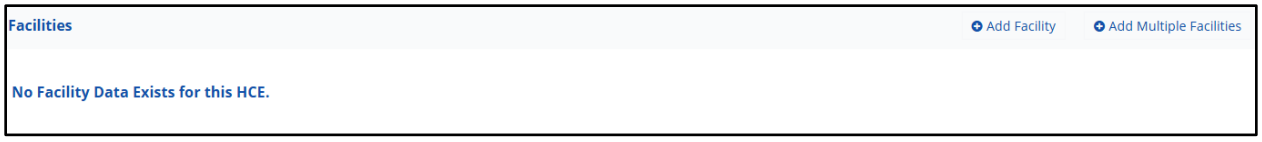
A screenshot of the *Show List* option is shown below and will only be displayed if the *Show List* button is clicked.

Clicking on a blue arrow transfers a role from the *Authorized Roles* list to the *Selected Roles* list. Clicking on an orange arrow transfers a role from the *Selected Roles* list to the *Authorized Roles* list.



9.2.5. Manage Facilities

This section provides details of the facilities related to this specific healthcare entity. These facilities and their active/ inactive statuses will be created and determined by the RxCheck PDMP Administrator or Super Administrator.



There are two buttons available to an RxConsole user.

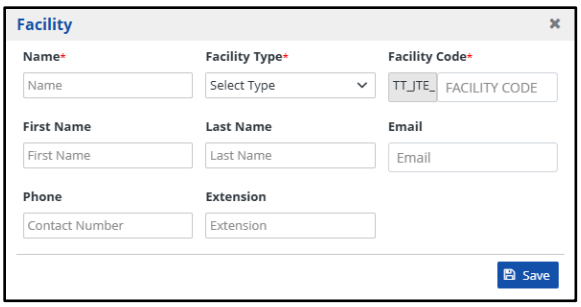
Button Name	Button Image	Functionality
Add Facility	Add Facility	Will display the *Facility* popup to enter a single facility.
Add Multiple Facilities	Add Multiple Facilities	Will redirect the PDMP administrator to the *Add Facilities* page.

9.2.5.1. How to add a single healthcare facility

1. Click on the *Add Facility* button.

2. In the pop-up window, enter the requested information in the appropriate data fields.

   To see a description of each field, see the table below.



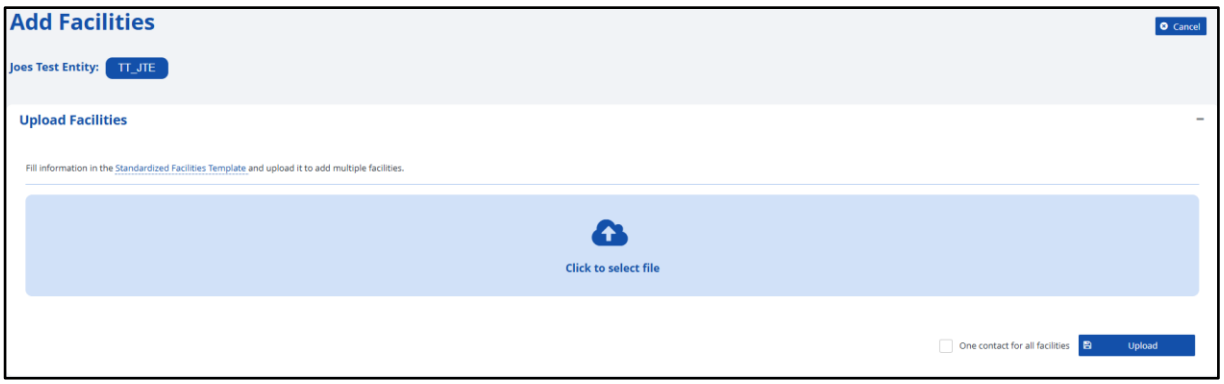
3. Click on the *Save* button to save the populated information.

Heading	Description
Name	Individual facility's name.
Facility Type	Individual facility type. Options include: • EHR – Electronic Health Record • PDS – Pharmacy Dispensing Software
Facility Code	Code specific to this individual facility. The HCE code is auto-populated, but the facility code is entered as an alphanumeric value.
First Name	Contact person's first name at this individual facility.
Last Name	Contact person's last name at this individual facility.
Email	Contact person's email at this individual facility.
Phone	Contact person's phone number at this individual facility.
Extension	Contact person's phone number extension at this individual facility, if any.

9.2.5.2. How to add multiple healthcare facilities

1. Click on the *Add Multiple Facilities* button.

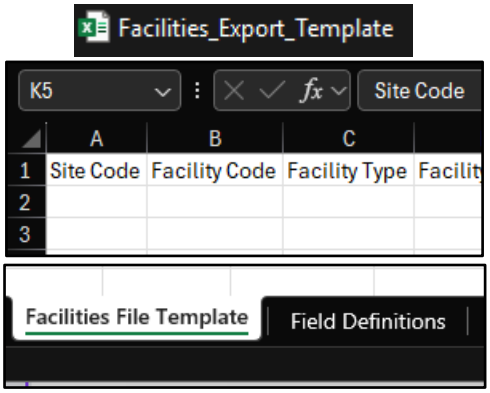
2. You will be directed to the *Add Facilities* screen.



3. Click on the *Standardized Facilities Template* link to download a template to populate. The template will download in an Excel workbook format (.xlsx).

   The first tab titled *Facilities File Template* contains columns to enter the same information available when adding a single facility. A table describing each heading is available in the previous subsection.

   The second tab titled *Field Definitions* provides an abbreviated summary of each field, its requirement status, and an example.



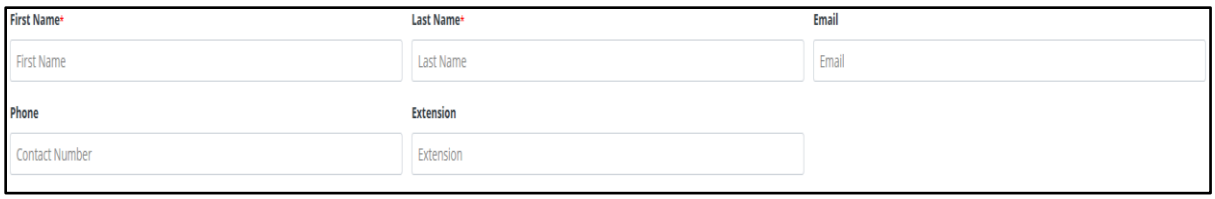
4. Populate the *Standardized Facilities Template* with each facility occupying a single row.

5. Press the *Click to select file* button to choose the populated template to upload into the system.

6. If all facilities share a single contact person, you can check the box labeled *One contact for all facilities* and data fields for that individual person will appear.

   A description of these fields can be found in the table in the previous subsection.

   Note: If contact information is included in both the uploaded data file and the UI (via "One contact for all facilities"), the UI entry will override and apply to all created facilities.

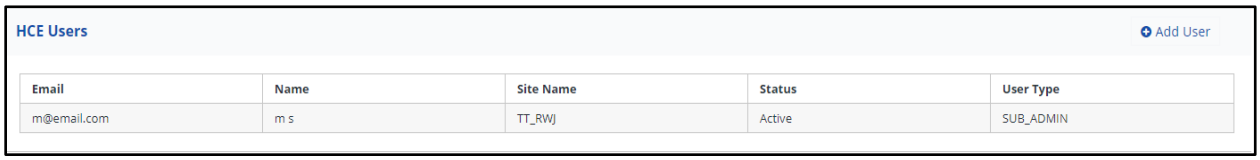


7. Click the *Upload* button to import the data populated in the file you selected in step 5.

8. The *Cancel* button will discard any changes made on this screen and return the user to the previous page.

9.2.6. User Administration

This section lists details of the administrator(s) specific to this healthcare facility.

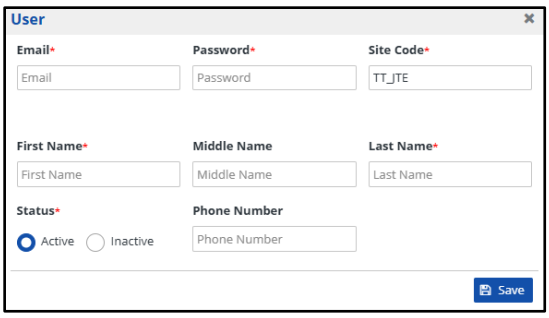


Heading	Description
Email	The email address used by the user to log into the RxConsole application.
Name	The first and last name of the HCE user.
Site Name	The HCE site code.
Status	The status of the HCE user account.
User Type	The type of account the HCE user has. This is typically displayed as *SUB_ADMIN*.

A State PDMP Administrator is allowed to add a new administrative user for a HCE following the steps below.

1. Click the *Add User* button to open a popup window.

2. In the popup window, enter the requested information into the appropriate data field.



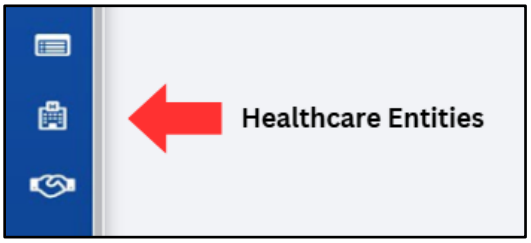
A description of each field is available in the following table.

3. Click the *Save* button to save the information populated in the fields.

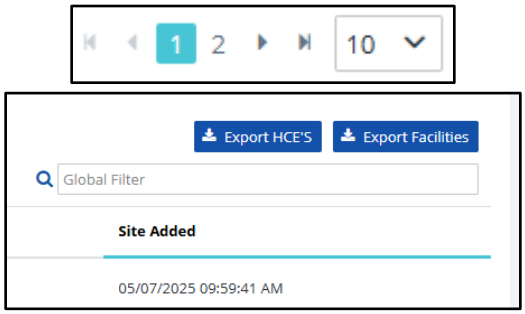
Heading	Description
Email	The contact email for the HCE user and username for RxConsole.
Password	The password for the HCE user to access the RxConsole application.
Site Code	The site code for the HCE user. This field will be auto-populated.
First Name	The HCE user's first name.
Middle Name	The HCE user's middle name.
Last Name	The HCE user's last name.
Status	The status of this HCE user's account. Can be set to either *Active* or *Inactive*.
Phone Number	The HCE user's phone number.

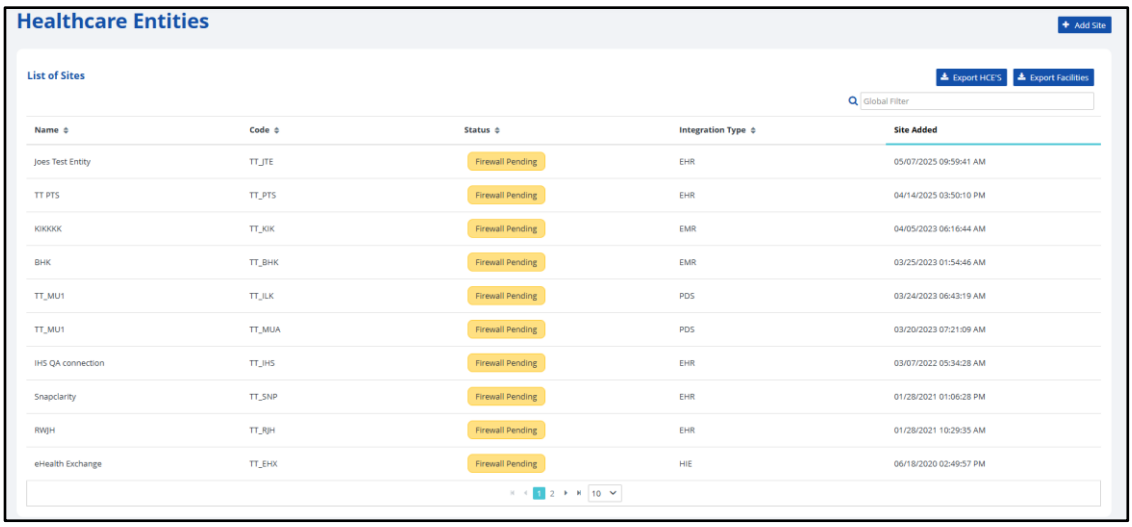
9.3. Open a healthcare entity record

1. Click on the *Healthcare Entities* button, located on the left-hand side of the screen.

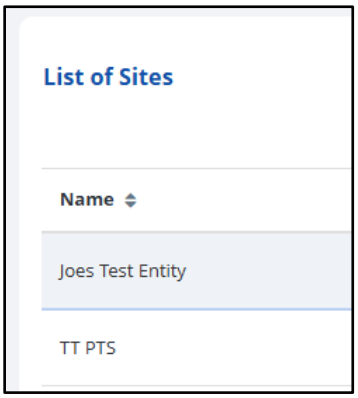


2. Find the healthcare entity using one of two methods:
   - Scroll through the list on the screen (may need to navigate to the next screen by using the navigation arrows at the bottom of the list)
   - Type the name of the HCE into the search bar labeled *Global Filter* in the top right.





3. Select the desired healthcare entity to view further details about that facility.

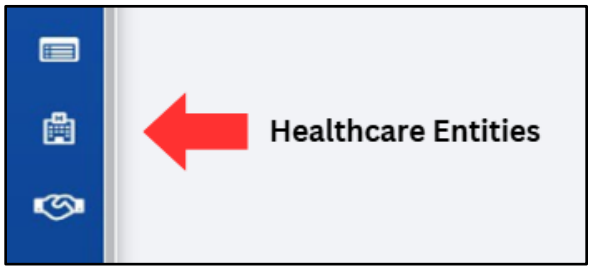


4. To edit a record, make your changes and click the *Save* button to ensure any new information is recorded.
   To exit without saving, click on the *Cancel* button.

9.4. Export a list of your HCE's and Facilities

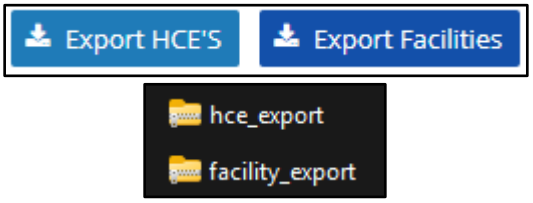
RxConsole supports the ability for a State PDMP Administrator to export a list of their healthcare entities and the facilities under those healthcare entities.

1. Click on the *Healthcare Entities* button, located on the left-hand side of the screen.

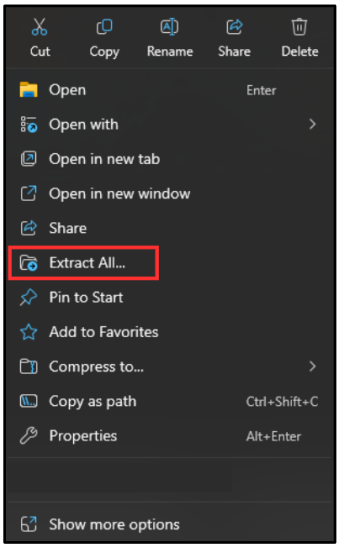


2. In the top-right corner, there are two buttons to extract either:
   - Export HCE'S—Downloads a list of healthcare entities, their HCE code, and their status.
   - Export Facilities—Downloads a list of Facilities, their site code, and their status.

   Note: The HCE and facility lists are downloaded in a zipped folder. Please see the tables in previous sections for a description of the columns in these files.



3. Right-click on the zipped folder to view options



4. Select the "Extract All…" option.

HCE Export Columns

Heading	Description
Code	A six-character code that follows the following format: • Two letters to represent the state code. • An underscore (_). • Three letters to represent a HCE site.
Name	The name of the Healthcare Entity.
Status	Status that indicates if a site is *Active* or *Inactive*.

Facility Export Columns

Heading	Description
Code	A facility code specific to that individual healthcare facility.
Name	The name of the facility.
Status	Status that indicates if the facility is *Active* or *Inactive*.

10. Interstate Data-sharing

The Interstate Data-Sharing feature enables State PDMP Administrators to designate which state are authorized to send prescription data requests to their PDMP and to restrict access from unauthorized states.

Only states that have executed a formal Memorandum of Understanding (MOU) can establish a secure digital connection via the RxCheck platform. These states must be designated as "Selected States" with the Interstate Data-Sharing portal by the State Administrator to enable bidirectional data-sharing.

States that have not finalized a formal agreement cannot participate in interstate data exchange through RxCheck. If such a state attempts to send a request, it will receive a system-generated message stating: "Access denied by disclosing state".

The screenshot below illustrates the configuration interface, showing the list of state authorized and unauthorized for interstate data-sharing.

Within the Interstate Data Sharing interface, two lists are displayed to manage site-level authorization:

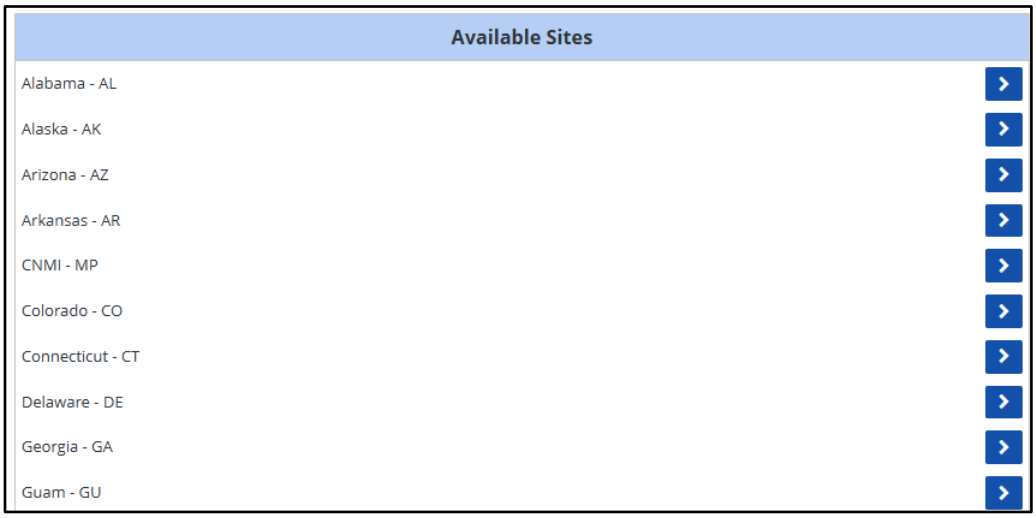
- Available Sites (left): This list displays PDMP sites that have not yet been authorized to connect with the host (disclosing) state. Sites in this list are unable to submit data requests to the host state, and any such attempts will result in failed transactions.
- Selected Sites (right): This list includes states that have been authorized to establish a bilateral connection with the disclosing state. These sites are permitted to send data requests and receive responses from the host PDMP system.

The following subsections provide step-by-step instructions for selecting and deselecting sites for interstate data sharing within the RxConsole Application. Each step is accompanied by a screenshot for visual reference.

10.1. Select states for interstate data-sharing

1. Click on the *Interstate Data Sharing* button, located on the left-hand side of the screen.

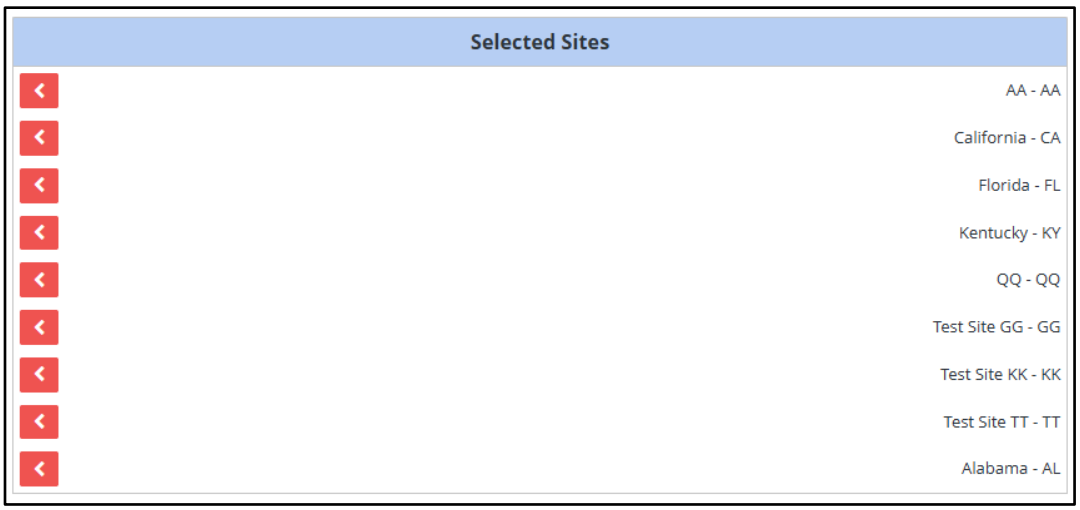
2. Scroll through the *Available Sites* list and locate the site you would like to add for interstate data-sharing.



3. Click on the blue arrow button aligned with the desired site.

4. Verify that the site has moved from the *Available Sites* list on the left to the *Selected Sites* list on the right.

   Note: Recently moved sites are not listed alphabetically and will instead appear at the bottom of the *Selected Sites* list.



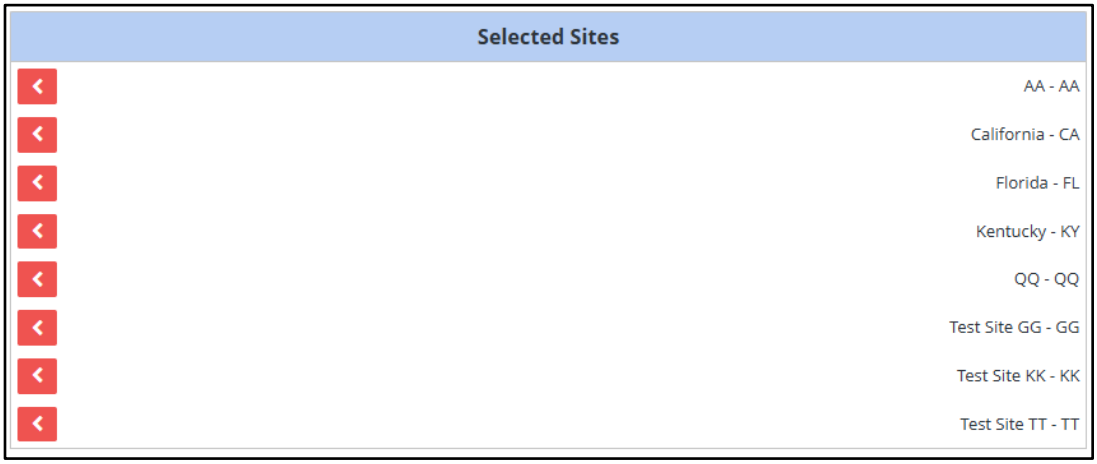
5. Click the *Save* button on the right corner of the screen to confirm and record your changes.

Note: If the change was implemented successfully, an alert will momentarily appear on the right-hand side of the screen with the message, "Alert – Selected Sites Saved"

10.2. Deselect states for interstate data-sharing

1. Click on the *Interstate Data Sharing* button, located on the left-hand side of the screen.

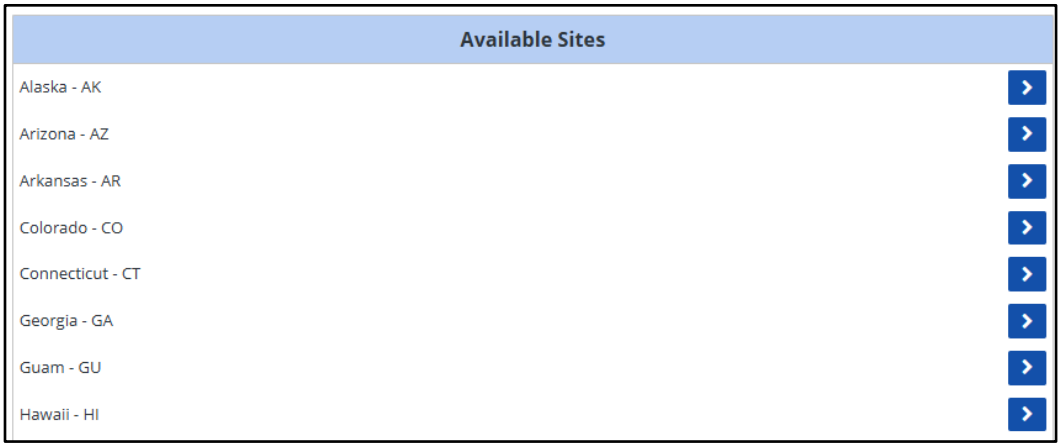
2. Scroll through the *Selected Sites* list and locate the site you would like to add for interstate data-sharing.



3. Click on the orange arrow button aligned with the desired site.

4. Verify that the site has moved from the *Selected Sites* list on the right to the *Available Sites* list on the left.

   Note: Recently moved sites are not listed alphabetically and will instead appear at the bottom of the Available *Sites* list.



5. Click the *Save* button on the right corner of the screen to confirm and record your changes.

   Note: If the change was implemented successfully, an alert will momentarily appear on the right-hand side of the screen with the message, "Alert – Selected Sites Saved"

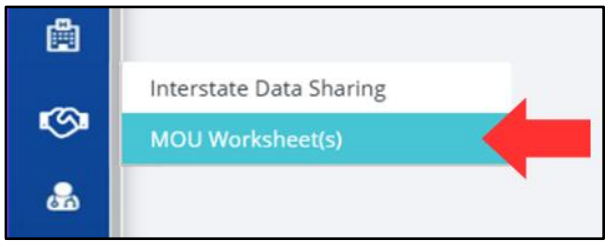
10.3. MOU Worksheet(s)

The RxConsole supports a Memorandum of Understanding (MOU) worksheet that states can populate and submit to potential partnering states. The partnering state also has the option to respond to an MOU worksheet submitted to them.

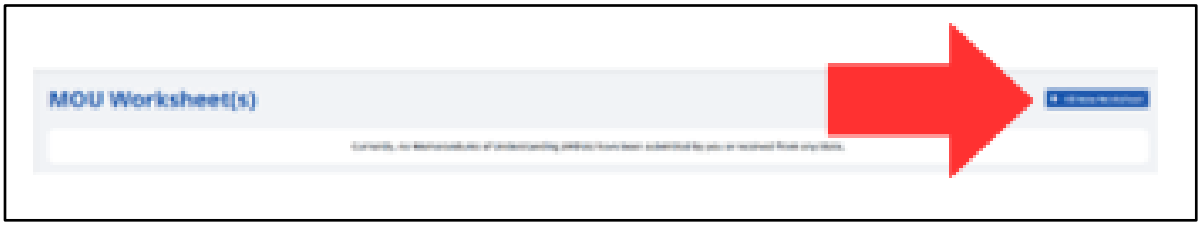
Note: This is an MOU worksheet, not a contract.

10.3.1 Populate and submit the MOU Worksheet

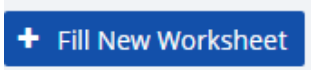
1. Click on the *Interstate Data Sharing* button, followed by the *MOU Worksheet(s)* option, located on the left-hand side of the screen.



2. The *MOU Worksheet(s)* page is displayed.



3. Click on the *Fill New Worksheet* button.

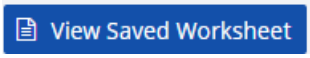


4. On the new *MOU Worksheet* page, populate the following:
   - State Administration's Information
   - User Validation Procedures
   - Data Access and Security
   - Data Elements for Request Submissions
   - Query Response
   - Miscellaneous

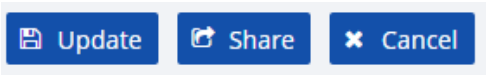
5. Click the *Save* button to confirm and record your changes to the MOU worksheet.

6. Alternatively, you can press the *Cancel* button to discard the changes and return to the previous screen.

7. After saving, the *View Saved Worksheet* button will be displayed.

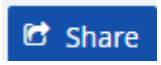


8. Click on *View Saved Worksheet* button to view the saved MOU Worksheet. PDMP Administrators can update the contents and/or share the MOU Worksheet with other state(s).

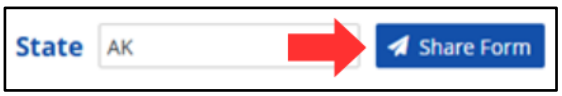


9. To edit the worksheet, click on the *Update* button.

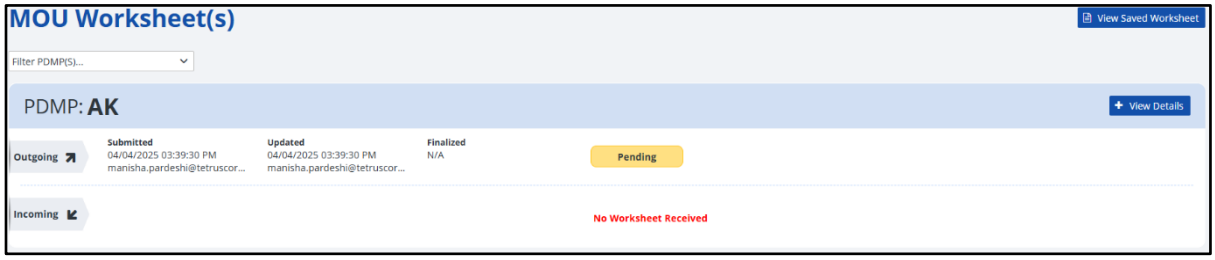
10. To share the worksheet with another state, click on the *Share* button.



11. Select a state from the dropdown menu and click the *Share Form* button to send the form to the selected state.

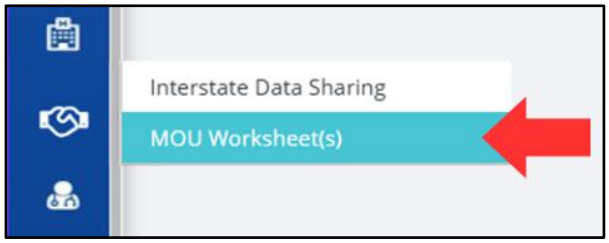


12. The MOU worksheet shared with the potential partnering state is displayed on the MOU Worksheet page with a “Pending”Status.

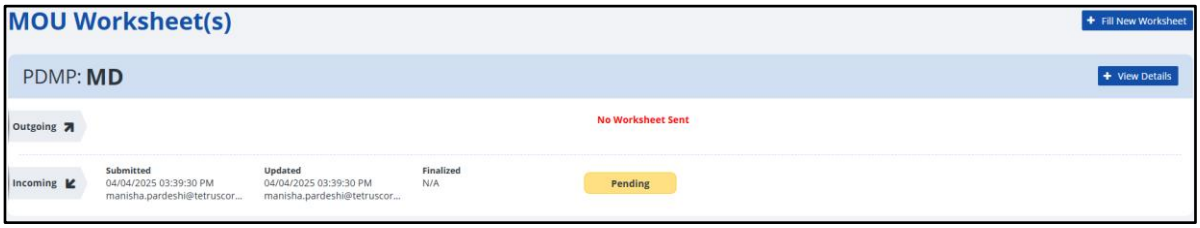


10.3.2. Review and respond to an MOU Worksheet submitted to your state

1. Click on the *Interstate Data Sharing* button, followed by the *MOU Worksheet(s)* option, located on the left-hand side of the screen.



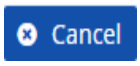
2. The MOU Worksheet(s) page is displayed with the MOU Worksheet record submitted by the PDMP State for Interstate Data Sharing Request.



3. Click on the *View Details* button to display the MOU Worksheet data submitted by the other PDMP State as view-only data.

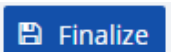
   Note: If the state that received the MOU Worksheet from another PDMP State has not filled out their MOU worksheet, they can do so by following the steps in the previous section titled, *Populate and submit the MOU Worksheet*.

4. Click the *Cancel* button to discard the MOU worksheet data.

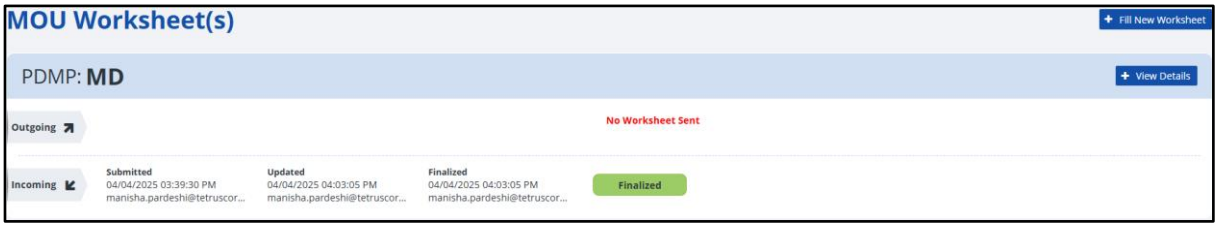


5. Click the *Print* button to print or save a copy of the MOU Worksheet.

6. To agree to the MOU Worksheet, click on the *Finalize* button.



7. The MOU Worksheet record will be displayed with a status of "Finalized" for both PDMP States.



11. Interstate Data-sharing – Role Management

The Role Management feature within the Interstate Data Sharing module enables State PDMP Administrators to control which user roles within an authorized state are permitted to submit prescription data requests for individual patients.

Administrators can selectively grant or restrict this capability based on the role designation of the requesting party.

The screenshot below displays two lists titled *Authorized Roles* and *Selected Roles* for the site "Florida-FL".

The *Authorized Roles* list (left) shows roles from Florida (FL) that do not have permission to request prescription data (e.g., *Homeopaths*, *Optometrists*). Users with these roles cannot send successful requests to the disclosing state.

The *Selected Roles* list (right) includes FL roles that are authorized for bilateral data exchange (e.g., *Pharmacists*, *Physicians*). Users with these roles can send and receive data successfully.

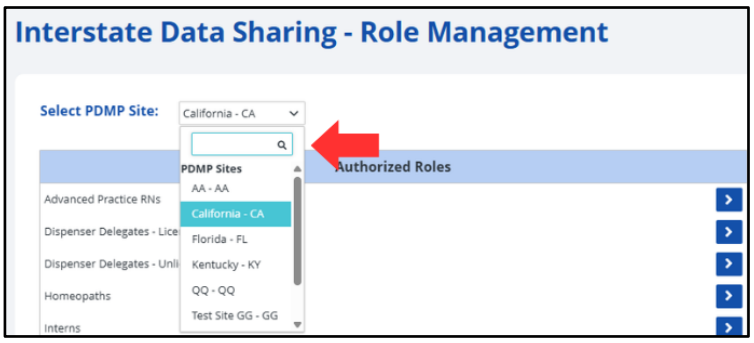
Note: These roles are standardized nationwide and based on the NCPDP Taxonomy Code list.

The following subsections contain step-by-step instructions on how to select and deselect roles for interstate data sharing in the RxConsole application. For additional clarity, each step is accompanied by a corresponding image or screenshot that depicts the action described.

11.1. Select roles for interstate data-sharing

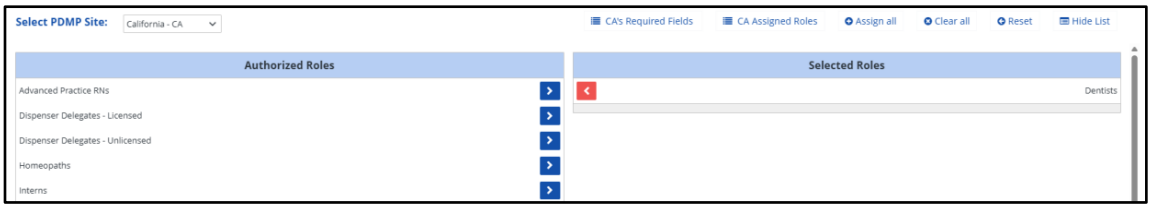
1. Click on the *Interstate Data Sharing – Role Management* button, located on the left-hand side of the screen.

2. Select the PDMP Site you would like to manage role for, by selecting the downward-facing arrow in the box labeled *Select PDMP Site:*. A user can find a site by:
   - Scrolling through the list in the dropdown, or
   - Entering the name or state code for the desired state in the dropdown search box.



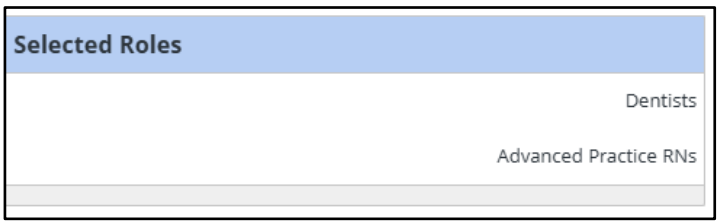
   Note: Only authorized sites from the Interstate Date Sharing section will be shown here as options.

3. Scroll through the list of *Authorized Roles* and locate the role you would like to add for Interstate Data Sharing.



4. Click on the blue arrow button aligned with the desired role.

5. Verify that the role has moved from the *Authorized Roles* list on the left to the *Selected Roles* list on the right.



   Note: Recently moved roles are not listed alphabetically and will instead appear at the bottom of the *Selected* Roles list.

6. Click the *Save* button on the right corner of the screen to confirm and record your changes.

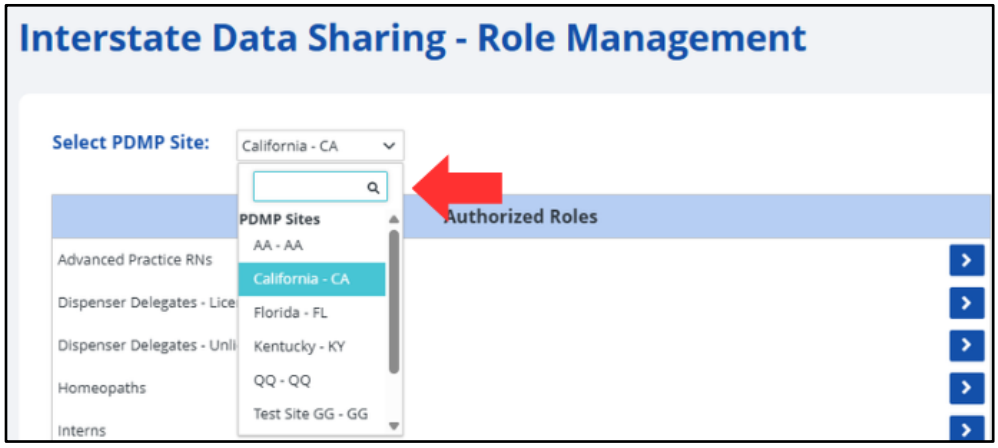
Note: If the change was implemented successfully, an alert will momentarily appear on the right-hand side of the screen with the message, "Alert – Selected Roles Saved"

11.2. Deselect roles for interstate data-sharing

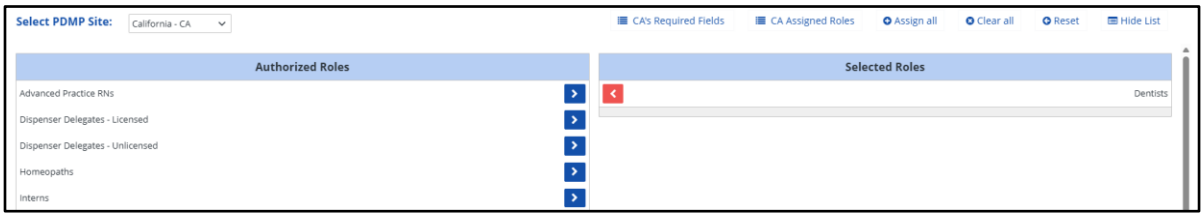
1. Click on the *Interstate Data Sharing – Role Management* button, located on the left-hand side of the screen.

2. Select the PDMP Site you would like to manage role for, by selecting the downward-facing arrow in the box labeled *Select PDMP Site:*. A user can find a site by:
   - Scrolling through the list in the dropdown, or
   - Entering the name or state code for the desired state in the dropdown search box.

   Note: Only authorized sites from the Interstate Date Sharing section will be shown here as options.



3. Scroll through the list of *Selected Roles* and locate the role you would like to remove from Interstate Data Sharing.



4. Click on the orange arrow button aligned with the desired role.

5. Verify that the role has moved from the *Selected Roles* list on the right to the *Authorized Roles* list on the left.

   Note: Recently moved roles are not listed alphabetically and will instead appear at the bottom of the Authoriz*ed* Roles list.

6. Click the *Save* button on the right corner of the screen to confirm and record your changes.

   Note: If the change was implemented successfully, an alert will momentarily appear on the right-hand side of the screen with the message, "Alert – Selected Roles Saved"

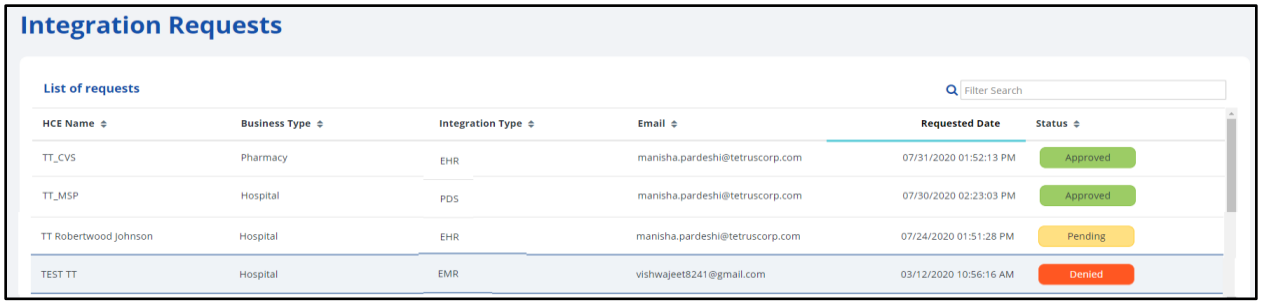
12. Integration Requests

The Integration Requests feature enables State PDMP Administrators to view and manage connection requests submitted by Healthcare Entities (HCEs) within their state.

Healthcare Entities interested in joining the RxCheck network must complete and submit the RxCheck HCE Integration Form. Once submitted, the request will appear in the state's RxConsole application under the Integration Requests section.

State PDMP Administrators are responsible for reviewing each request to determine the eligibility of the HCE for participation in the RxCheck network. Based on this review, the administrator may choose to approve or deny the integration request.

The screenshot below shows a list of integration requests received by a PDMP state system. The accompanying table provides detailed definitions of each column heading presented in the interface.



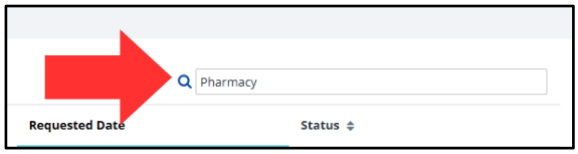
Heading	Description
HCE Name	The name of the healthcare entity.
Business Type	The business type of the healthcare entity. For example, Hospital or Pharmacy.
Integration Type	The integration type requested by the healthcare entity. For example, NCPDP.
Email	The business email of the healthcare entity for communication purposes.
Requested Date	The date and time that the HCE integration request was submitted.
Status	The current state of the HCE integration request. For example, Approved, Pending, or Denied.

The following subsection contains step-by-step instructions on how to view and search for integration requests in the RxConsole application. For additional clarity, each step is accompanied by a corresponding image or screenshot that depicts the action described.

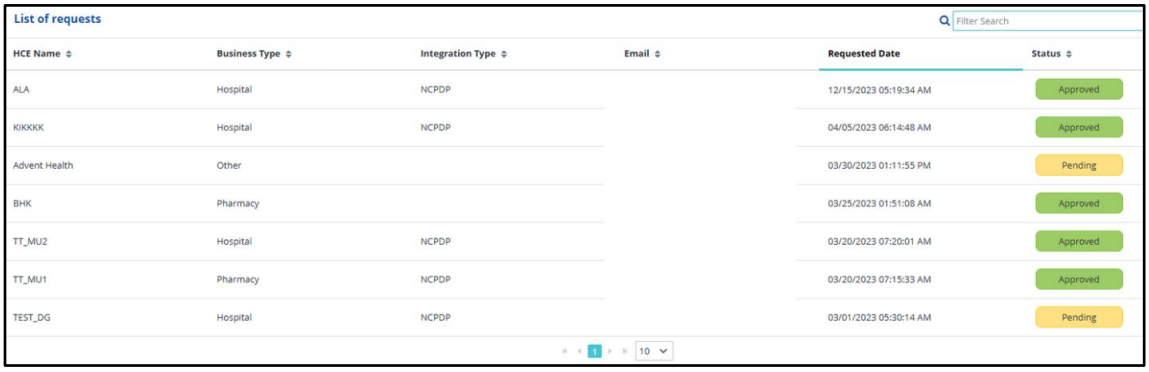
12.1. Search for integration requests

1. Click on the *Integration Requests* button, located on the left-hand side of the screen.

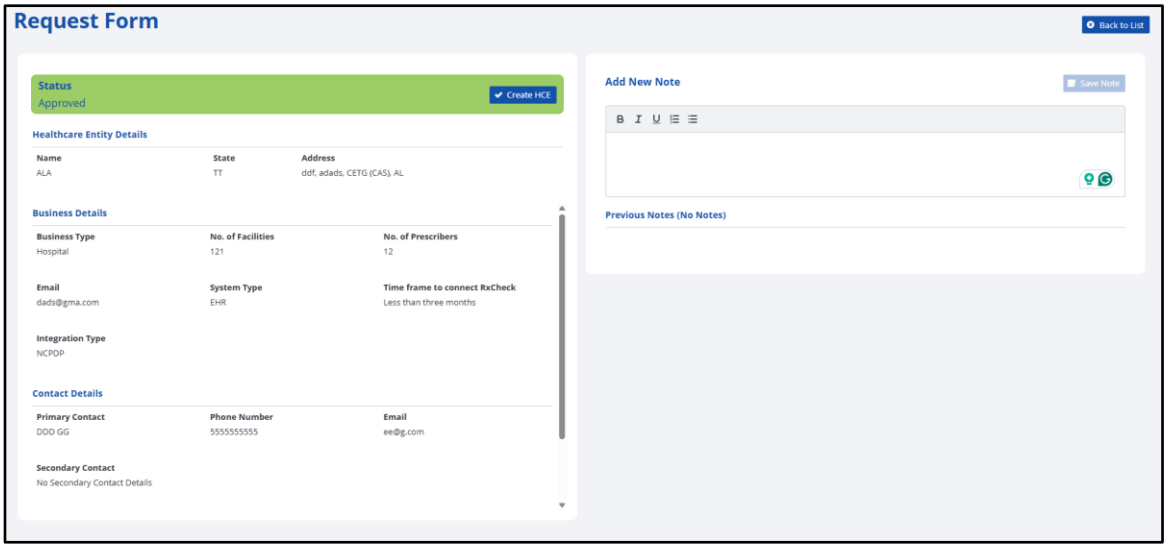
2. Locate the integration request you are searching for by either:
   - Scrolling through the listed requests, or
   - Searching for the facility in the *Filter Search* bar.



Note: You can search for information under any of the columns. For example, searching for "Pharmacy" will show all integration requests with the Business Type of Pharmacy.

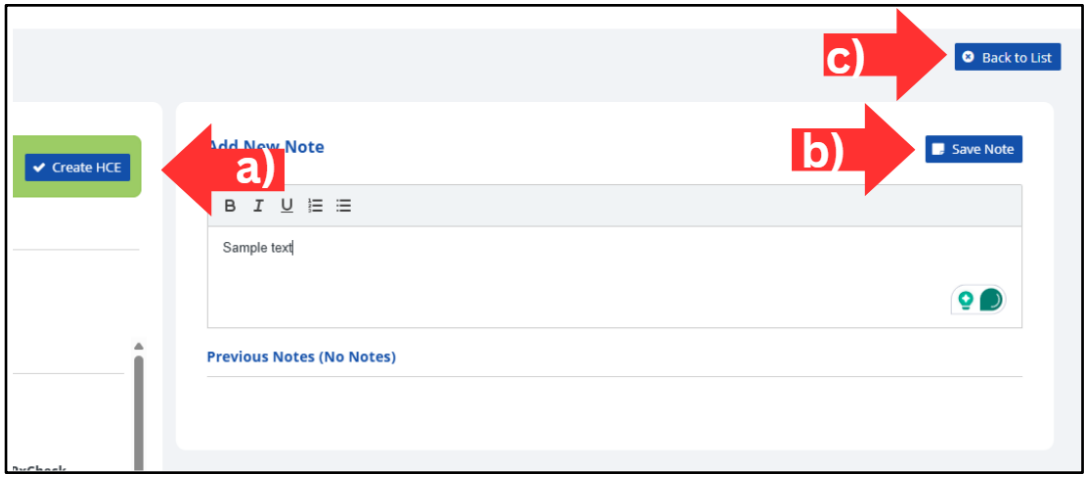


3. Click on a desired integration request to view further details regarding the request. A request form which contains details regarding the status, healthcare entity, business details, contact information, and other related integration information will be displayed.



4. In addition to viewing additional details, you can also perform the following options:
   a. Create a new healthcare entity from the information included in the request by clicking the *Create HCE* button.
   b. Add a new note to the integration request by typing into the text box labeled *Add New Note* and then clicking on the *Save Note* button.

   Return to the integration list by clicking the *Back to List* button.

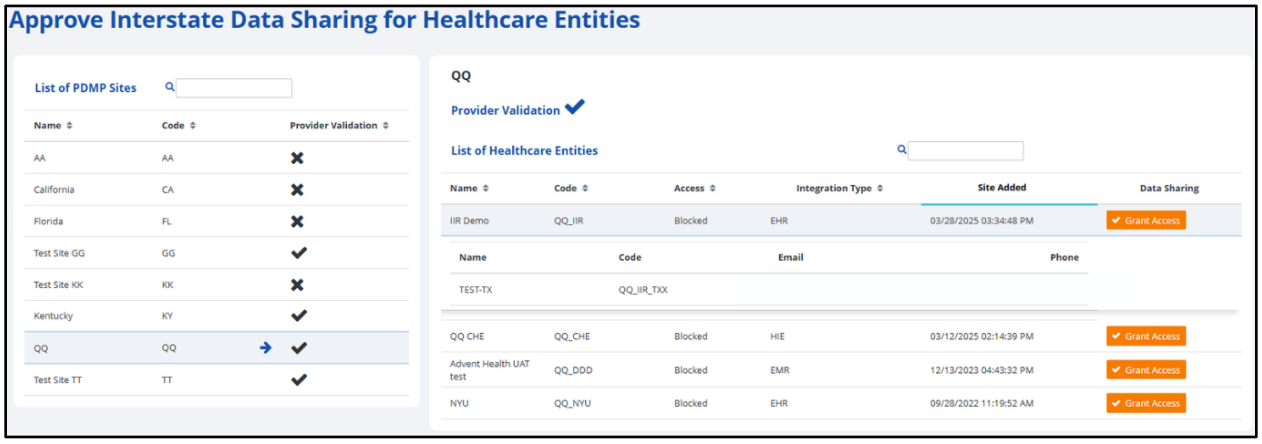


13. Approving interstate data-sharing for healthcare entities

This feature enables State PDMP Administrators to grant or deny interstate data sharing access to individual Healthcare Entities (HCEs) within any state that has an established bilateral data sharing agreement.

Upon selecting a site, the administrator will see a list of HCEs associated with that site, along with their respective site configuration details. The administrator can then review each entity and determine whether to authorize it for interstate data-sharing with the administrator's state.

The screenshot below shows an example list of HCEs associated with the site "QQ". Selecting a healthcare entity reveals an expanded view displaying the site's configuration and facility information. The accompanying table provides definitions for each column heading shown in the screenshot.



Heading	Description
Name	The name of the PDMP site.
Code	The site code associated with the PDMP site.
Provider Validation	An icon indicating if that PDMP site has provider validation enabled in RxConsole. An **X** indicates that provider validation is disabled for this site, while a ✓ indicates that provider validation is enabled.

Heading	Description
Name	The name of the healthcare entity.
Code	The site code of the healthcare entity.
Access	The access level granted to the HCE by the PDMP state for interstate data-sharing.

Heading	Description
Integration Type	The integration / site type of the HCE, such as EHR, EMR, HIE, or PDS.
Site Added	The date and time when the HCE was added.
Data Sharing	The options to grant or deny access to the HCE for interstate data-sharing permissions.
Expanded Line – Name	The name of the facility under the selected HCE record.
Expanded Line – Code	The facility code of the facility record.
Expanded Line – Email	The email address of the facility for communication purposes.
Expanded Line – Phone	The phone number of the facility.

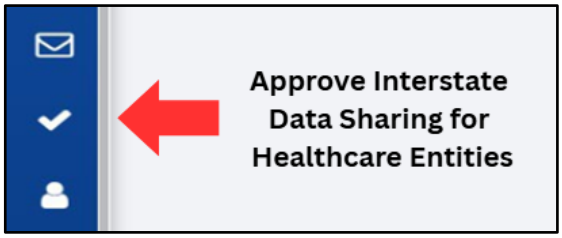
If a healthcare entity shows a blue *Deny Access* button under Data Sharing, it currently has interstate data sharing access. Clicking the button will revoke this access.

If it shows an orange *Grant Access* button, the entity does not have access. Clicking it will grant interstate data sharing permission.

The following subsection contains step-by-step instructions on how to approve interstate data sharing for healthcare entities in the RxConsole application. For additional clarity, each step is accompanied by a corresponding image or screenshot that depicts the action described.

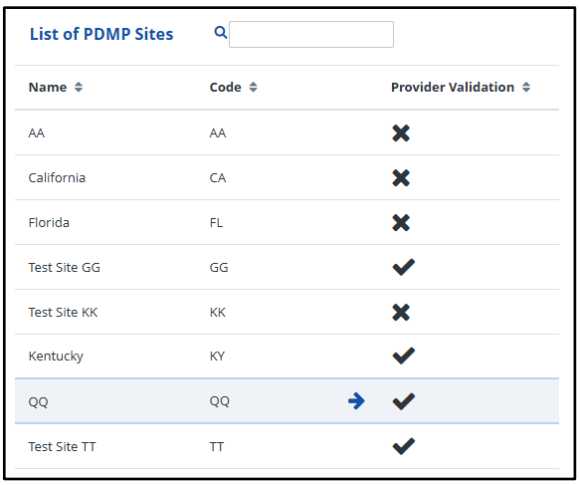
13.1. Approve or revoke interstate data-sharing requests

1. Click on the *Approve Interstate Date Sharing for Health Entities* button, located on the left-hand side of the screen.



2. Select a PDMP site from the list of PDMP sites, located on the left side of the screen.

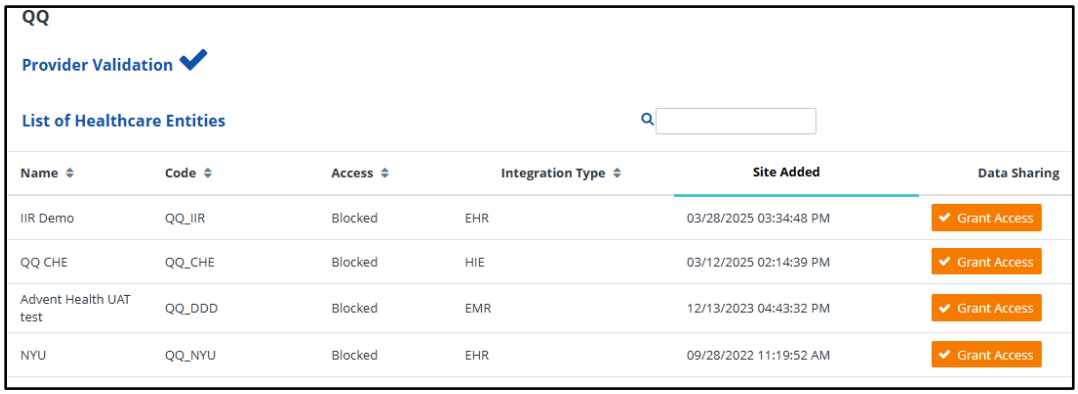
   Note: QQ has been selected for demonstration purposes.



List of PDMP Sites

Name	Code	Provider Validation
AA	AA	✗
California	CA	✗
Florida	FL	✗
Test Site GG	GG	✓
Test Site KK	KK	✗
Kentucky	KY	✓
QQ	QQ	✓
Test Site TT	TT	✓

3. Review the list of HCE's associated with the selected site, as displayed on the right-side of the screen.



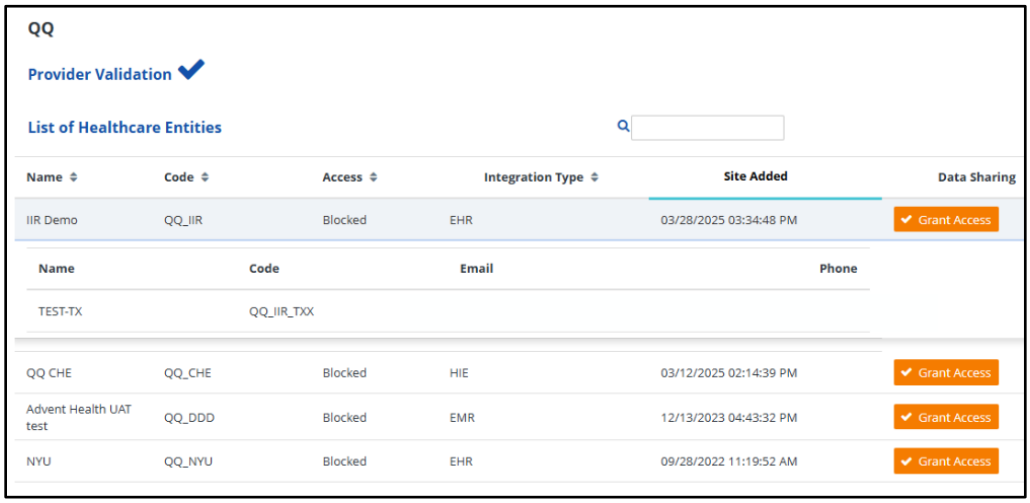
QQ

Provider Validation ✓

List of Healthcare Entities

Name	Code	Access	Integration Type	Site Added	Data Sharing
IIR Demo	QQ_IIR	Blocked	EHR	03/28/2025 03:34:48 PM	Grant Access
QQ CHE	QQ_CHE	Blocked	HIE	03/12/2025 02:14:39 PM	Grant Access
Advent Health UAT test	QQ_DDD	Blocked	EMR	12/13/2023 04:43:32 PM	Grant Access
NYU	QQ_NYU	Blocked	EHR	09/28/2022 11:19:52 AM	Grant Access

4. Click on a healthcare entity to view expanded details relating to its site configuration and facilities data.



QQ

Provider Validation ✓

List of Healthcare Entities

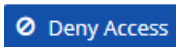
Name	Code	Access	Integration Type	Site Added	Data Sharing
IIR Demo	QQ_IIR	Blocked	EHR	03/28/2025 03:34:48 PM	Grant Access

Name	Code	Email	Phone
TEST-TX	QQ_IIR_TXX		

QQ CHE	QQ_CHE	Blocked	HIE	03/12/2025 02:14:39 PM	Grant Access
Advent Health UAT test	QQ_DDD	Blocked	EMR	12/13/2023 04:43:32 PM	Grant Access
NYU	QQ_NYU	Blocked	EHR	09/28/2022 11:19:52 AM	Grant Access

5. Grant or revoke data-sharing access to a healthcare entity by:
   a. Pressing the orange *Grant Access* button to enable interstate data-sharing for that site, or
   b. Pressing the blue *Deny Access* button to disable interstate data-sharing access for that site.

i.

ii. 

6. Verify that your action has been successfully implemented by looking for the following alerts:
   c. If access was granted, an alert that states "Site Unblocked Successfully", or
   d. If access was revoked, an alert that states "Site Blocked Successfully"

i.

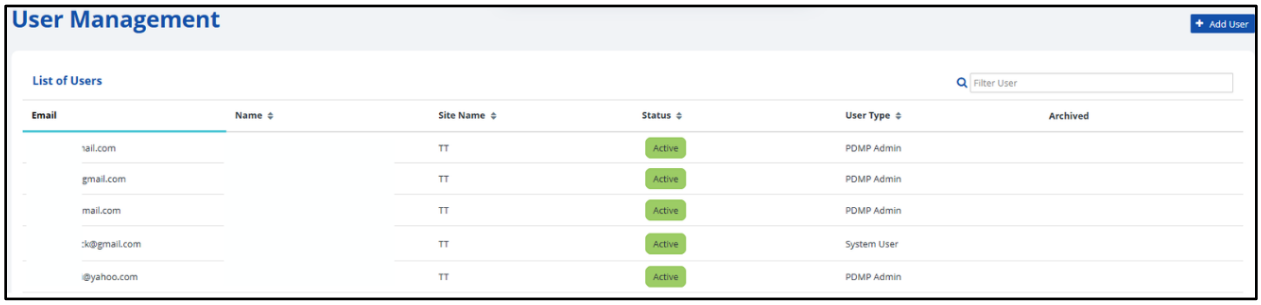
ii.

14. User Management

State PDMP Administrators are responsible for managing user access within their systems. This includes the ability to add new users with the user type “System User”.

In addition, State Administrators can view a list of existing PDMP Administrators and System Users, and they have the authority to edit details for current System Users. However, to modify information related to an existing PDMP Administrator, the State Administrator must submit a request to the RxCheck Administrator.

The screenshot below displays a sample list of PDMP Administrators and System Users for the test site “TT”. The accompanying table provides descriptions for each column heading shown in the interface.



Heading	Description
Email	The email address used to log into the RxConsole application.
Name	The first and last name of the user.
Site Name	The name of the site for which the user has been created.
Status	The status of the user, either *Active* or *Inactive*.
User Type	The type of user. For example, PDMP Admin or System User.

The following subsections contain step-by-step instructions on how to manage users in the RxConsole application. For additional clarity, each step is accompanied by a corresponding image or screenshot that depicts the action described.

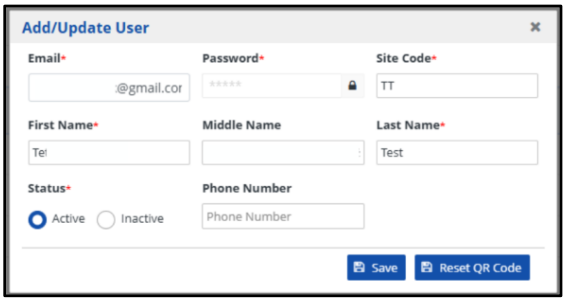
14.1. Search for and update user information

1. Click on the *User Management* button, located on the left-hand side of the screen.

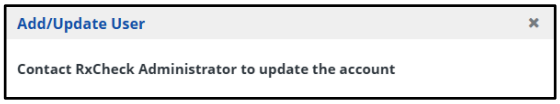
2. Locate the user you are searching for by:
   a. Scrolling through the list of users displayed on the screen, or
   b. Searching for a user by typing his / her name into the *Filter User* search bar in the top right corner of the screen.

3. Select the desired user by clicking on their information to view or modify their existing record.
   a. If the user type is **System User**, a pop-up screen titled *Add/Update User* will appear.
   b. If the user type is **PDMP Admin**, a pop-up notification will appear to inform the user to reach out the RxCheck Administrator.

a)



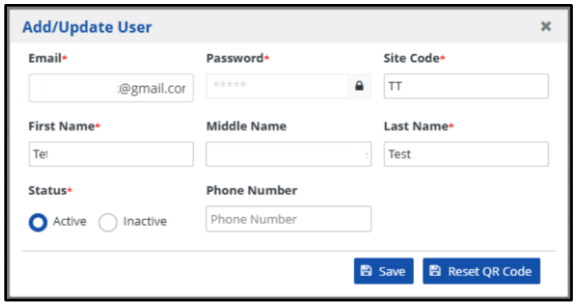
b)



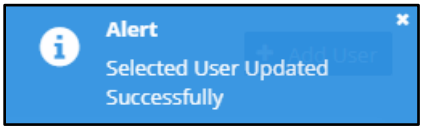
4. For system users, you may edit any information (except the password) displayed in each data field.

   Note: If you change any information, remember to click the *Save* button to record the changes. Alternatively, pressing the *X* in the top right will discard any changes made and exit the window.

   Note: Refer to the following table for a description of each data field.



5. Verify that the user has been successfully updated by looking for the alert that states, "Selected User Updated Successfully".

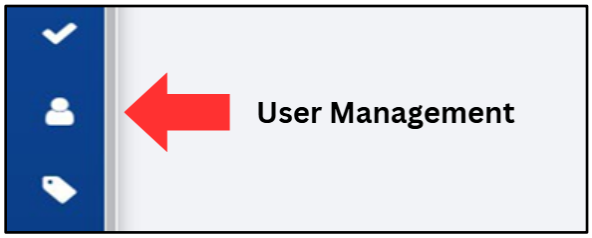


Heading	Description
Email	The contact email for the HCE user and username for RxConsole.
Password	The password for the HCE user to access the RxConsole application.
Site Code	The site code for the HCE user. This field will be auto-populated.
First Name	The HCE user's first name.
Middle Name	The HCE user's middle name.
Last Name	The HCE user's last name.
Status	The status of this HCE user's account. Can be set to either *Active* or *Inactive*.
Phone Number	The HCE user's phone number.

Note: See the Section titled, *User Roles and Privileges in the RxConsole Application* for more information about the different user roles available.

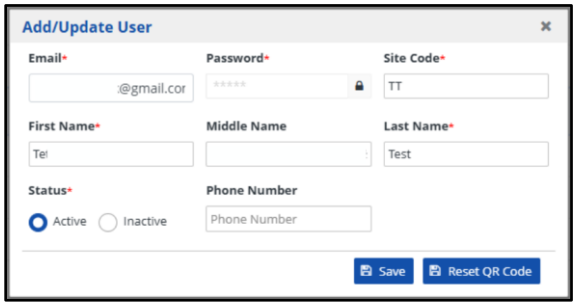
14.2. Adding users

1. Click on the *User Management* button, located on the left-hand side of the screen.



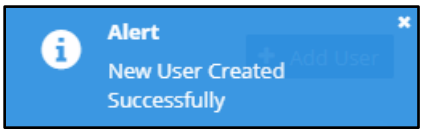
2. Click on the *Add User* button located in the top right corner of the screen.

3. In the popup window, enter the requested information into the appropriate data field.
   a. A description of each field is available in the table at the end of the previous section.



4. Click on the *Save* button on the pop-up window to record the information added to your new user.

5. Verify that the new user has been successfully added by looking for the alert that states, "New User Created Successfully".



15. Provider Validation

The term "Provider" refers to a licensed healthcare professional or organization legally authorized to deliver medical services to the public. Federal regulations recognize a wide range of provider types, including pharmacies, physicians, and nurse practitioners.

Most providers in the US are uniquely identified by a 10-digit National Provider Identifier (NPI), issued by the Centers for Medicare and Medicaid Services (CMS). Additionally, the Drug Enforcement Agency (DEA) in the US also assigns practitioners with a DEA Registration Number, authorizing them to prescribe controlled substances. Providers must also hold a valid state license, evidenced by a State License Number (SL#) specific to the state in which they practice.

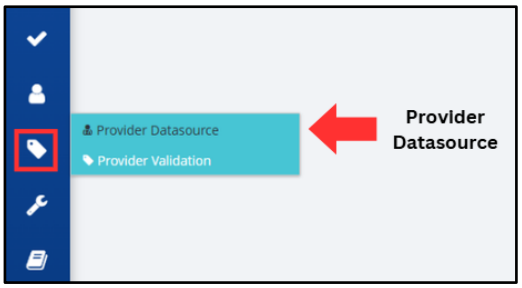
Whenever a healthcare entity sends or receives a prescription data request via RxCheck, the provider's NPI, DEA, and/or SL# is included in the data payload.

The Provider Validation feature in RxConsole allows State PDMP Administrators to configure whether the validation of the NPI, DEA, and/or SL# is required, optional, or not validated prior to processing a request.

The screenshot below displays the available NPI and DEA validation options. The following section explains each option in detail.

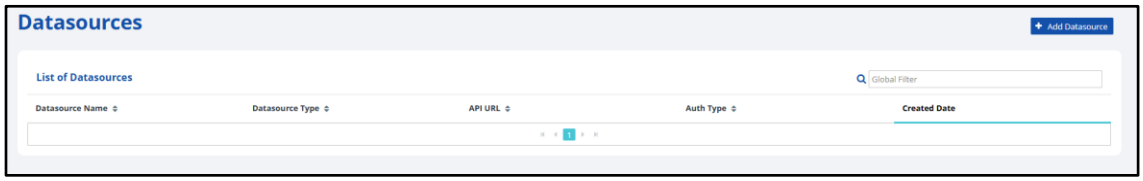
15.1. View and add a datasource for provider validation

1. Click on the Provider *Management* button, followed by the *Provider Datasource* option, located on the left-hand side of the screen.



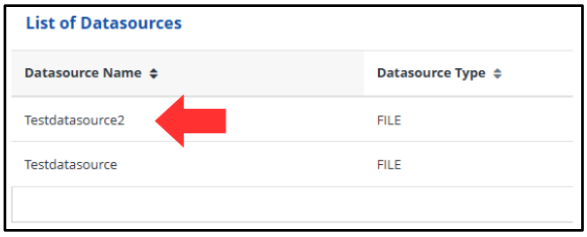
2. The Datasources screen allows you to view previously uploaded datasources.

   Refer to the following table for a description of each column header.



3. To add a new provider datasource, press the *Add Datasource* button.
   For instructions on adding a new datasource, see the subsection titled, *Add a new Datasource file* later in this guide.

4. To view a previously entered datasource, click on a datasource name in the *List of Datasources*.

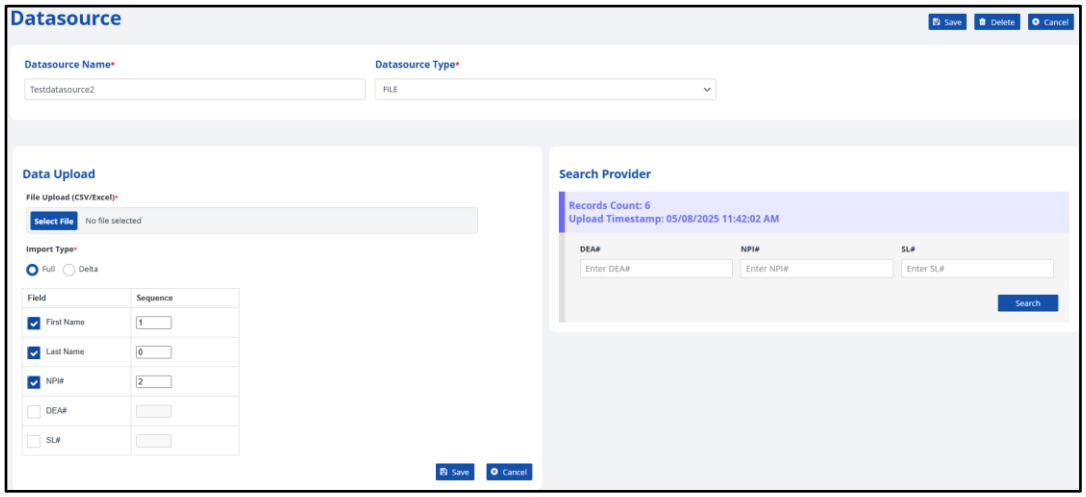


Header	Description
Datasource Name	The name entered by the PDMP administrator referencing this unique datasource.
Datasource Type	Identifies the datasource type as a File or API.
API URL	The URL for the API to call for provider identification.
Auth Type	The authorization method for calling the API.
Created Date	The date and time the datasource was added into the RxConsole.

15.2. View, modify, delete, and search an existing datasource

1. Follow steps 1, 2, and 4 under the section titled *View and add a datasource for provider validation* in this guide to view an existing datasource.

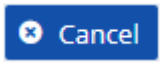
2. The new screen will look similar to the *Add Datasource* screen, but includes a section labeled *Search Provider*.



2. To modify an existing datasource, simply enter any changes on the view datasource screen.
   a. In this screen, we can upload a new datasource file and select the "Import Type" as *Delta*. This allows us to update the existing datasource with only the changes between the existing datasource and the new file.

3. After making any changes, click on the *Save* button to record any changes.

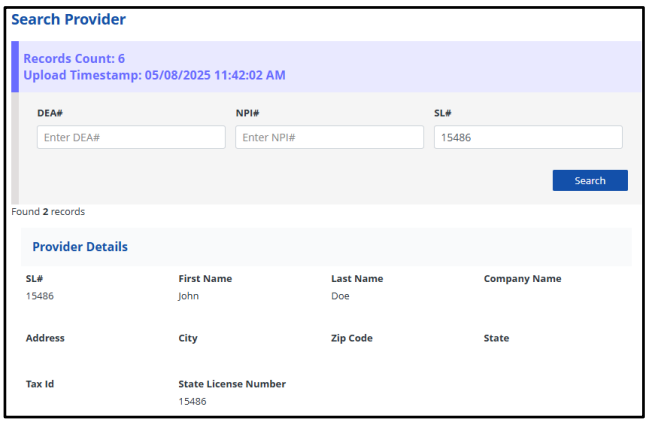
4. Alternatively, if you do not wish to proceed with your changes, you can press the *Cancel* button to discard the changes and return to the previous screen.



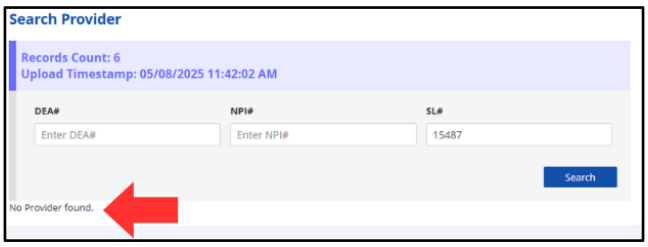
5. If you wish to remove a datasource, you can press the *Delete* button.

6. To see if an existing datasource file contains a provider, you can enter the DEA#, NPI#, or SL# in the *Search Provider* section to see if that provider exists on the datasource you are viewing.
   a. If the provider is on the list, you will see their information returned under the *Search Provider* section.
   b. If the provider is not on the list, you will see "No Provider found." Under the *Search Provider* section.

a)



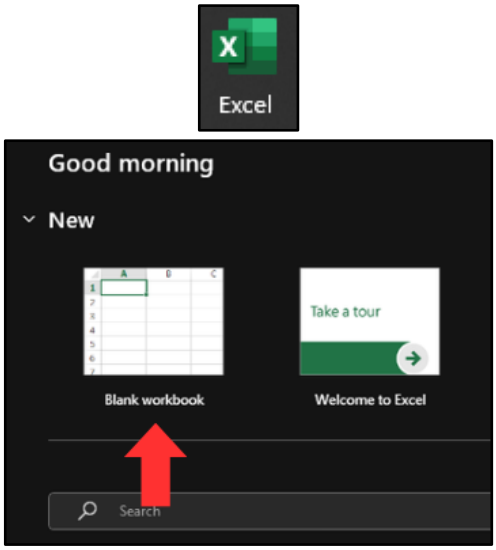
b)



Note: The datasource search feature is only available for datasource files and cannot be used on a datasource API.

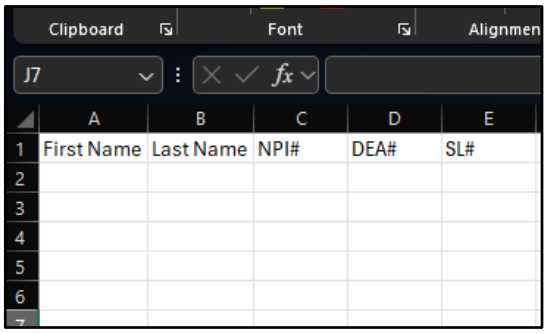
15.2.1. Create a datasource file

1. Open Microsoft Excel on your computer.



2. Create a new blank workbook.

3. Add your desired headers in any order you prefer. The names of the possible headers are:
   - First Name
   - Last Name
   - NPI#
   - DEA#
   - SL#



Note: The header names should be entered in cells A1, B1, C1, D1, and E1.

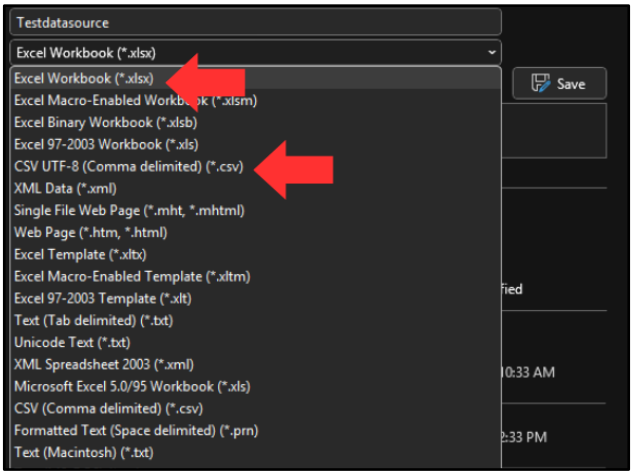
Note: Not all header names are required and any combination of headers can be used (For example, if a state administrator does not want to use the DEA number, the may elect to remove that header completely.

4. Populate the relevant information under the corresponding column.

   Note: Duplications in the First Name and Last Name column are expected and will not affect provider validation.

	A	B	C	D	E
1	First Name	Last Name	NPI#	DEA#	SL#
2	John	Doe	1234567890	AD1236547	15486
3	John	Doe	1345678901	BD1265478	51234
4	Jane	Doe	1564875630	BD5987401	65432

5. When finished building your datasource file, save the file as either a .csv (Comma Separated Values (CSV)) or .xlsx (Excel workbook).



15.2.2. Add a new datasource file

1. Follow steps 1-3 under the section titled [*View and add a datasource for provider validation*](#) in this guide.

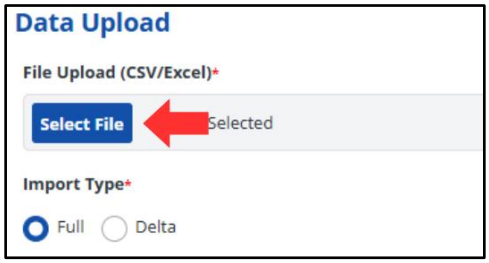
2. Select the "File" option under the *Datasource Type* dropdown.

   Note: Selecting the *File* option, allows a PDMP administrator to upload a .csv (CSV) or .xlsx (Excel workbook) .

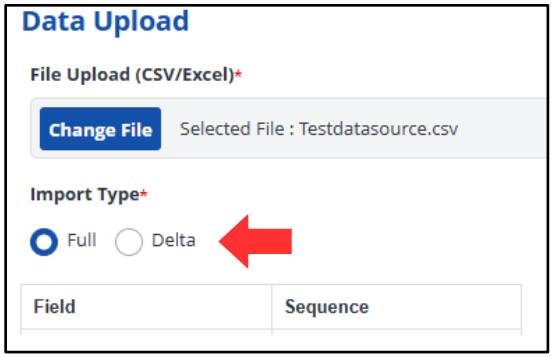
3. Enter a name for your datasource file in the text field labeled, *Datasource Name*.

   Note: The name does not need to match your datasource file. The name in this field can be up to 15 alphanumeric characters (Spaces and special characters are not allowed).

4. Press the *Select File* button under the *Data Upload* section.
   a. Find your datasource file using the system dialog window.



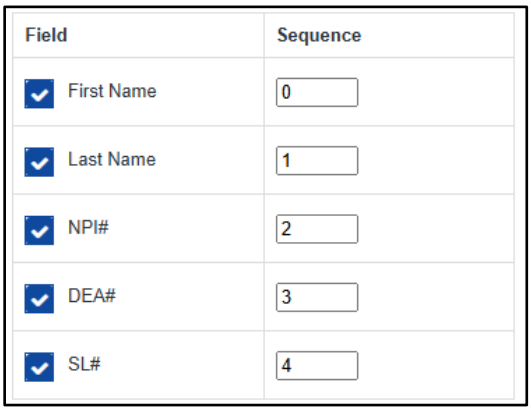
5. Select your import type:
   a. Full – will import the entire datasource file under the name you entered in step 3.
   b. Delta – this is only successful when viewing a previous datasource (see previous section titled, [*View and add a datasource for provider validation*]() for instructions to view a previous datasource).



6. Check the fields that are present in your datasource file. If you did not include a field, you can leave box unchecked.
   a. After checking the box, you will need to set the sequence. This refers to the order of the columns in your datasource file.

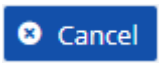
   Note: Column A is sequence "0", Column B is sequence "1", etc.

   Example: Using step 3 from the previous subsection, you can see how the sequence is populated in the screenshot for this step.



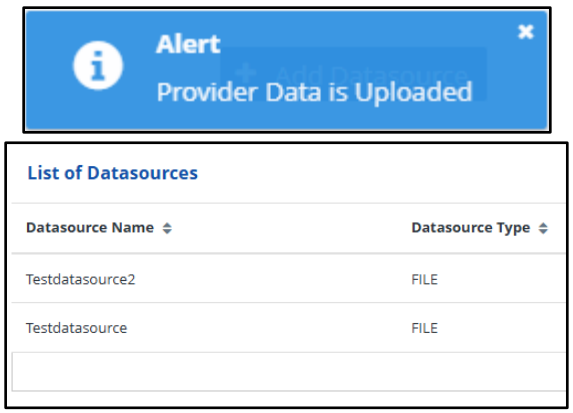
7. Press the *Save* button on the right corner of the screen to add your datasource file to the RxConsole for your state.

8. Alternatively, if you do not wish to add your data source you can press the *Cancel* button to discard changes and return to the previous screen.



9. Verify your datasource file was successfully added by looking for the Alert that states, “Provider Data is Uploaded”

   You will also return to the Datasource screen and should see your datasource in the *List of Datasources*.



15.2.3. Add a datasource API

1. Follow steps 1-3 under the section titled *View and add a datasource for provider validation* in this guide.

2. Select the “API” option under the *Datasource Type* dropdown.

3. Enter the API URL into the field labeled *API URL*.

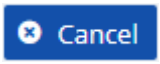
4. Select the appropriate authorization type using the *Auth Type* dropdown.

5. For BASIC authorization, enter the username and password.

6. For OAUTH2 authorization, enter the Client ID, Client Secret, and Auth URL into their respective fields.

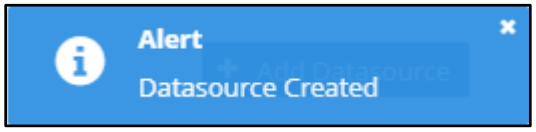
7. Press the *Save* button on the right corner of the screen to add your datasource API to the RxConsole for your state.

8. Alternatively, if you do not wish to add an API you can press the *Cancel* button to discard changes and return to the previous screen.



9. Verify the datasource API was successfully added by looking for the Alert that states, "Datasource Created".

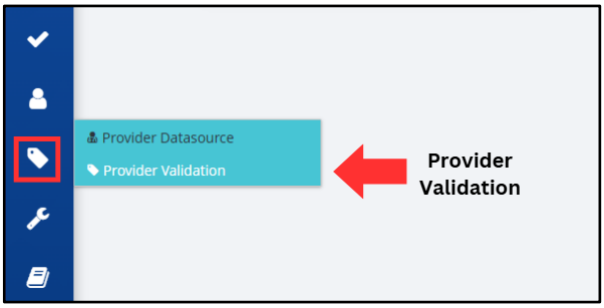
   You will also return to the Datasource screen and should see your datasource in the *List of Datasources*.



15.3. Configure provider validation options

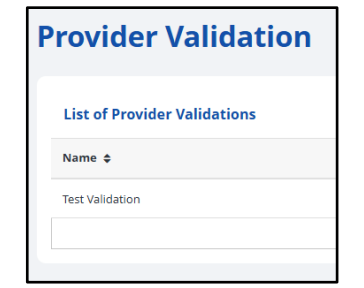
15.3.1. Modify an existing provider validation

1. Click on the *Provider Management* button, followed by the *Provider Validation* option, located on the left-hand side of the screen.

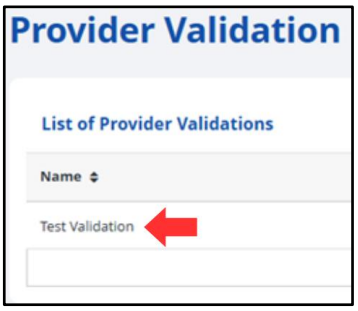


2. The Provider Validation screen allows you to view a list of existing validations that have been added and includes a button to add a new provider validation.

   Note: The names of the headers are described in the table following these steps.

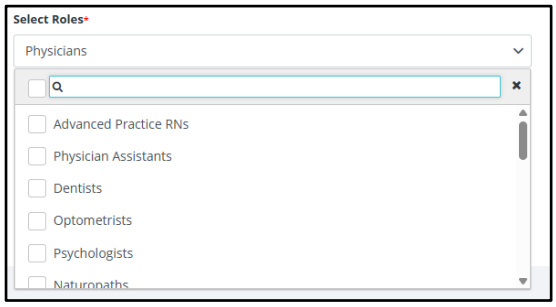


3. To view and/or modify an existing validation, click on the name of a validation.



4. The following screen allows you to change settings related to the existing validation.
   a. Name – change the name of the validation settings.
   b. Select Roles – change the roles that are subject to validation.
   c. Validation Type – if *Mandatory* is chosen, a query will fail if the fields are not present, while Validate will stop a query if the validation check fails.
   d. Datasource – allows you to select a datasource to reference for the validation check. (Only present if validate is chosen for the *Validation Type*.)
   e. Selection – if *All* is chosen, all boxes checked in the *Validation Field(s)* selection will be checked for validation. If *Any* is chosen, only one of the numbers must pass for the validation to be successful.
   f. Validation Field(s) – allows you to check which ID numbers are subject to validation.

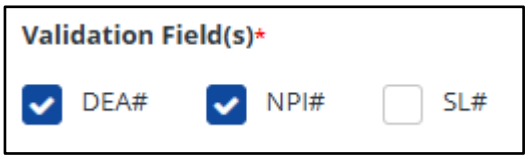
a)

b)


c)

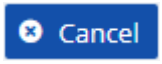
d)

e)

f)


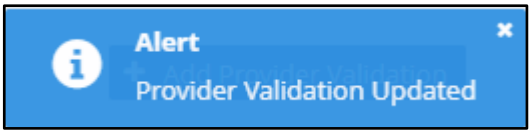
5. Press the *Save* button on the right corner of the screen to record your changes to provider validation to the RxConsole for your state.

6. Alternatively, if you do not wish to proceed with your changes, you can press the *Cancel* button to discard changes and return to the previous screen.



7. Verify the Provider Validation was successfully updated by looking for the Alert that states, “Provider Validation Updated”.

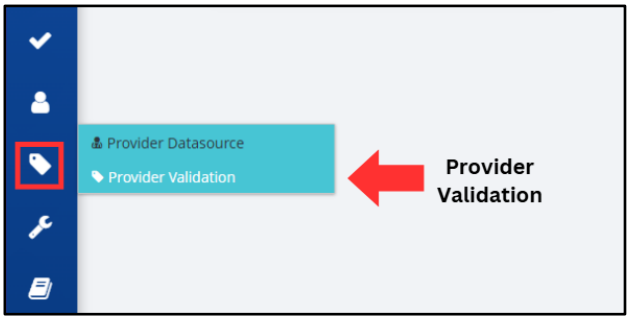
   You will also return to the Provider Validation screen and should see your changes in the *List of Provider Validations*.



Header	Description
Name	The name given to this specific set of validation rules.
Datasource Name	The name of the datasource that is referenced for validation.
Validation Fields	The identification numbers that are subject to validation.
Validate Type	The type of validation occurring, Mandatory will stop a query if the fields are not present, while Validate will stop a query if the validation check fails.
Created Date	The date and time the validation rules were created.

15.3.2. Add a new provider validation

1. Click on the *Provider Management* button, followed by the *Provider Validation* option, located on the left-hand side of the screen.



2. To add a new set of validation rules, click on the *Add Provider Validation* button.

3. The following screen allows you to add settings related to the new validation rules.
   a. Name – assigns a name to the validation settings.
   b. Select Roles – add the roles that are subject to validation. Clicking

a)

the checkbox next to the search box will select/deselect all.

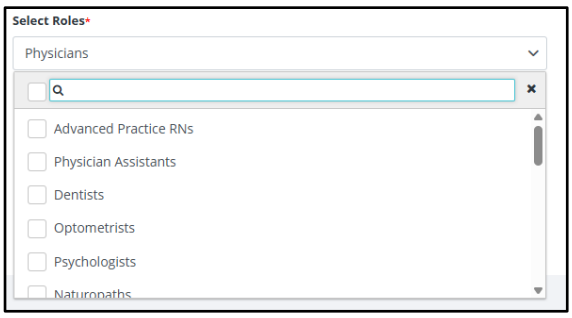
c. Validation Type – if *Mandatory* is chosen, a query will fail if the fields are not present, while Validate will stop a query if the validation check fails.

d. Datasource – allows you to select a datasource to reference for the validation check. (Only present if validate is chosen for the *Validation Type*.)

e. Selection – if *All* is chosen, all boxes checked in the *Validation Field(s)* selection will be checked for validation. if *Any* is chosen, only one of the numbers must pass for the validation to be successful.

f. Validation Field(s) – allows you to check which ID numbers are subject to validation.

b)

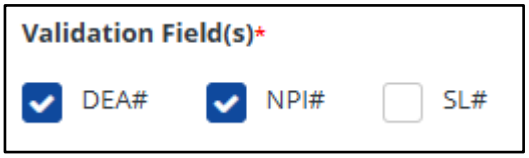


c)

d)

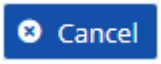
e)

f)



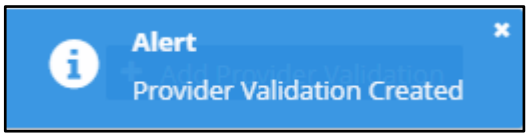
4. Press the *Save* button on the right corner of the screen to add your new provider validation rules to the RxConsole for your state.

5. Alternatively, if you do not wish to proceed, you can press the *Cancel* button to discard changes and return to the previous screen.



6. Verify the Provider Validation was successfully created by looking for the Alert that states, “Provider Validation Created”.

   You will also return to the Provider Validation screen and should see your new rules in the *List of Provider Validations*.

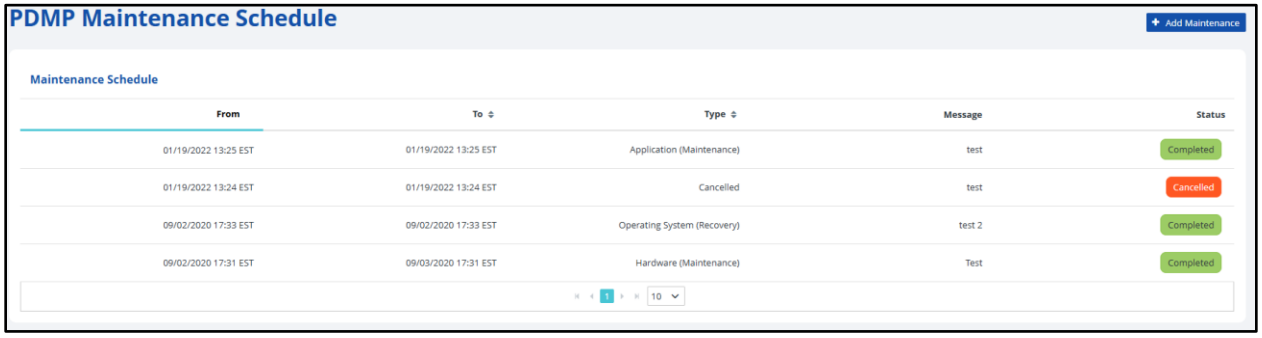


16. PDMP Maintenance Schedule

The Maintenance Schedule feature in RxConsole enables State PDMP administrators to create and manage scheduled maintenance events. These events may include activities such as application updates, software installations, or operating system configurations.

During a maintenance window, the PDMP system will be taken offline, meaning it will not be able to process incoming requests or generate responses. If a request is received during this time, the system will return an error code “DM”, indicating a processing error due to scheduled maintenance. Once the maintenance period concludes, the system will resume normal operations and process all pending and new requests.

The screenshot below shows an example Maintenance Schedule for a test site, “TT”. The accompanying table provides descriptions for each column heading displayed in the interface.

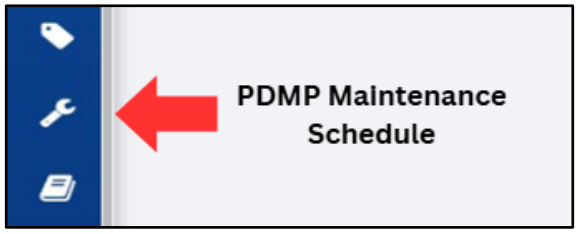


Heading	Description
From	The date and time for when the maintenance event will begin.
To	The date and time for when the maintenance event will end.
Type	The event type for which the maintenance event is scheduled.
Message	The user can add an informative note about the respective event.
Status	The status of the scheduled event, such as “Completed” or “Cancelled”.

The following subsection contains step-by-step instructions on how to add a PDMP maintenance schedule entry in the RxConsole application. For additional clarity, each step is accompanied by a corresponding image or screenshot that depicts the action described.

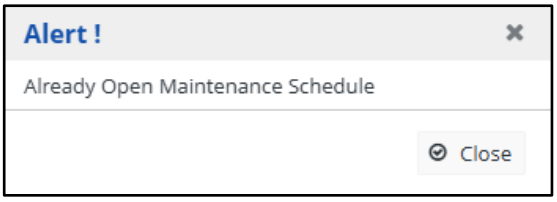
16.1. Create and modify a maintenance event

1. Click on the *PDMP Maintenance Schedule* button, located on the left-hand side of the screen.

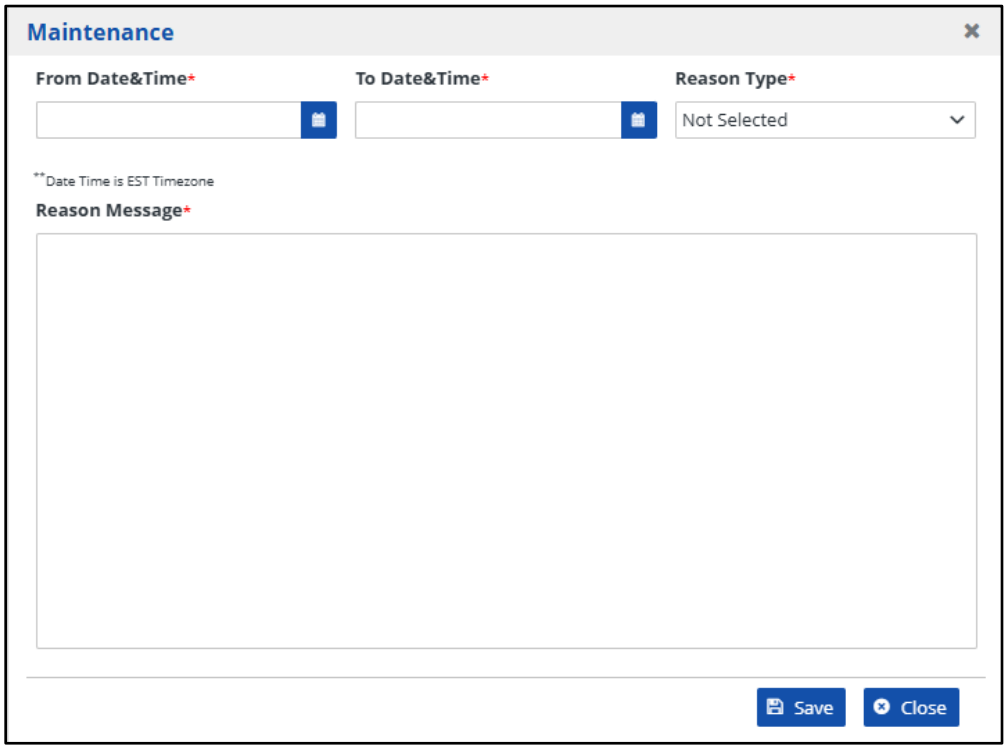


2. Click on the *Add Maintenance* button located on the top right-hand corner of the screen.

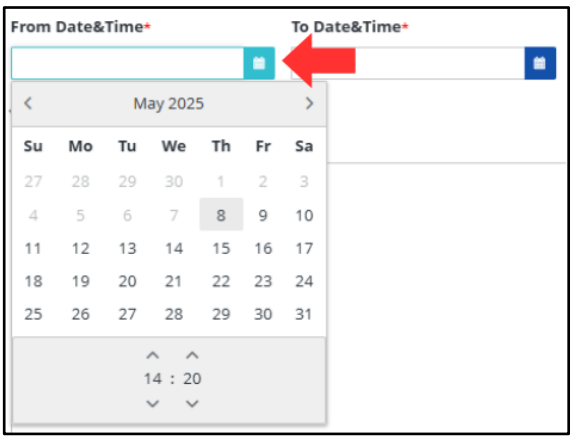
Note: You can only create a new maintenance event if no other upcoming event is scheduled. If there's a conflict, an alert message will appear.



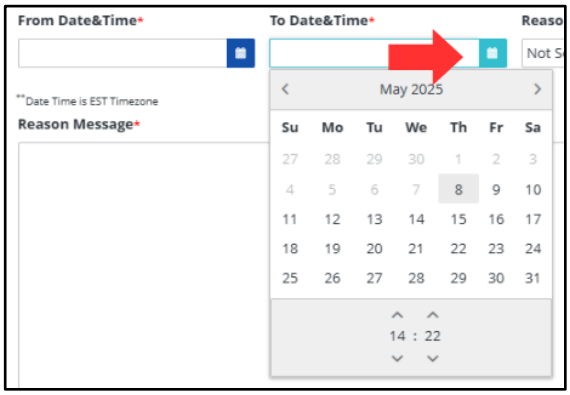
3. A pop-up screen titled *Maintenance* will appear.



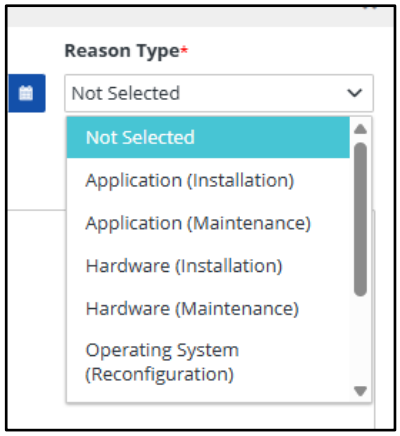
4. Select the start date and time by making appropriate selections in the calendar by clicking the blue calendar in the field labeled *From Date&Time*.



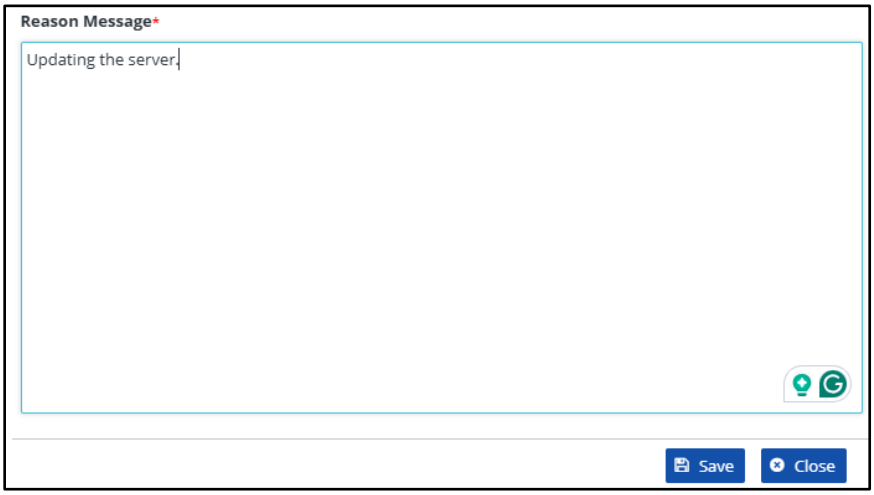
5. Select the end date and time by making appropriate selections in the calendar by clicking the blue calendar in the field labeled *To Date&Time*.



6. Select the reason for the maintenance event by clicking on one of the dropdown options for the field labeled, *Reason Type*.



7. Add a note into the text box labeled, *Reason Message* to add context to the maintenance event.

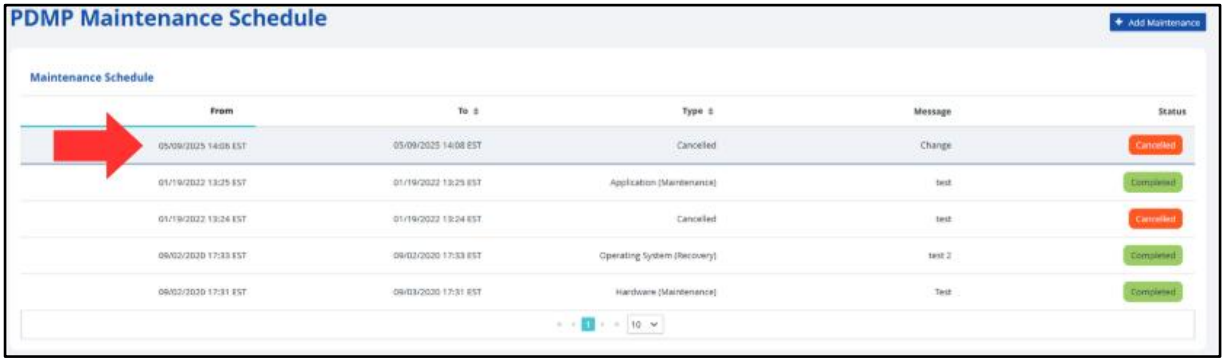


8. Press the *Save* button to add the new maintenance event to the maintenance schedule in the RxConsole.

9. Alternatively, you can press the *Close* button to discard changes and return to the previous screen.

To modify an already existing maintenance event.

10. Click on an event listed in the *Maintenance Schedule*.



11. Modify any information in the *Maintenance* popup similar to if you were adding a new event.

12. Press the *Save* button to record the changes to the maintenance event in the RxConsole.

13. Alternatively, you can press the *Close* button to discard changes and return to the previous screen.

14. Press the *Complete* button to mark the event as completed.

15. Press the *Cancel* button to cancel the event in the maintenance schedule.

17. NCPDP Taxonomy Code Mapping

Taxonomy codes are 10-character alphanumeric identifiers used to classify healthcare providers and organizations based on the primary services they offer. These codes are assigned at both the individual and organization provider levels are used to represent the provider's type, classification, and specialization for claim-level identification.

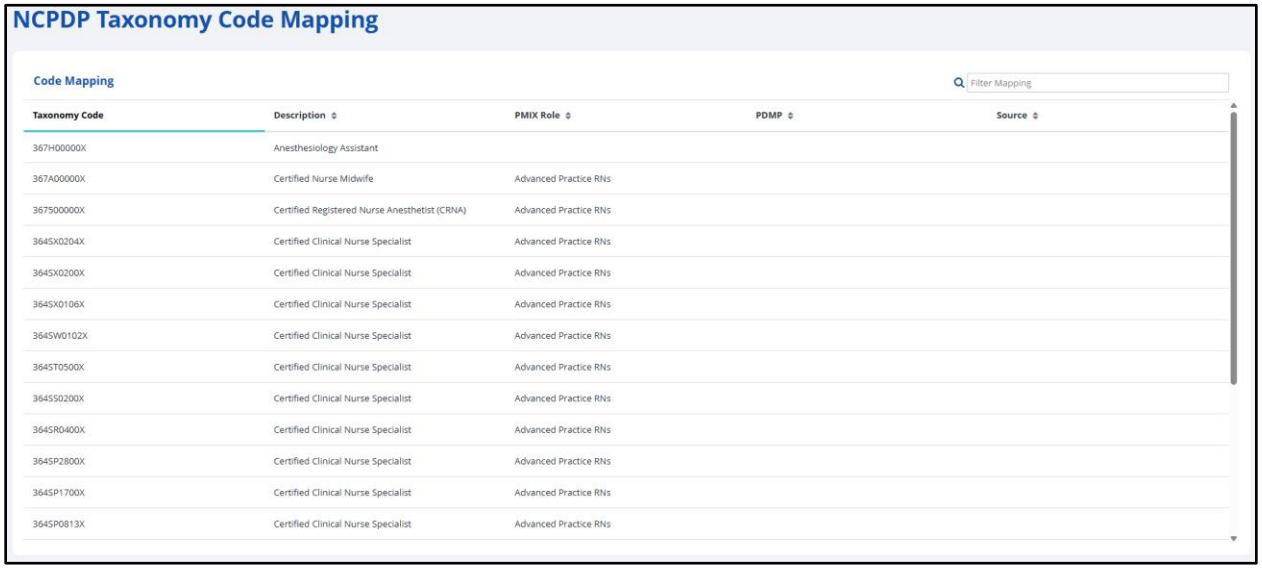
The taxonomy code structure consists of three hierarchical levels:

1. Provider Type
2. Classification
3. Specialization

Each successive level adds greater specificity. All taxonomy codes are 10 characters long and end with the letter "X". The first four characters represent the Level 2 Classification, while the middle 5 characters vary depending on the Level 3 Specialization.

Within the RxCheck application, the roles configured in the *Interstate Data Sharing* and *Role Management* sections are derived from the NCPDP Taxonomy Code Mapping list. State PDMP Administrators can browse the complete list or search for specific codes or roles as needed.

The screenshot below shows a sample page from the NCPDP Taxonomy Code Mapping list. The accompanying table provides detailed descriptions for each column heading displayed in the screenshot.



NCPDP Taxonomy Code Mapping

Code Mapping

Filter Mapping

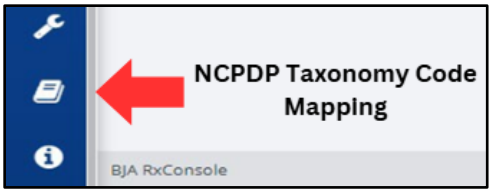
Taxonomy Code	Description	PMIX Role	PDMP	Source
367H00000X	Anesthesiology Assistant			
367A00000X	Certified Nurse Midwife	Advanced Practice RNs		
367500000X	Certified Registered Nurse Anesthetist (CRNA)	Advanced Practice RNs		
364SX0204X	Certified Clinical Nurse Specialist	Advanced Practice RNs		
364SX0200X	Certified Clinical Nurse Specialist	Advanced Practice RNs		
364SX0106X	Certified Clinical Nurse Specialist	Advanced Practice RNs		
364SW0102X	Certified Clinical Nurse Specialist	Advanced Practice RNs		
364ST0500X	Certified Clinical Nurse Specialist	Advanced Practice RNs		
364SS0200X	Certified Clinical Nurse Specialist	Advanced Practice RNs		
364SR0400X	Certified Clinical Nurse Specialist	Advanced Practice RNs		
364SP2800X	Certified Clinical Nurse Specialist	Advanced Practice RNs		
364SP1700X	Certified Clinical Nurse Specialist	Advanced Practice RNs		
364SP0813X	Certified Clinical Nurse Specialist	Advanced Practice RNs		

Heading	Description
Taxonomy Code	Administrative codes set for identifying the provider type and area of specialization for health care providers. They consist of ten alphanumeric characters always terminating with the letter "X."
Description	A brief description of the Healthcare Professional Role displayed for that taxonomy code.
PMIX Role	The PMIX role that the corresponding taxonomy code is mapped to.
PDMP	The PDMP state for which the taxonomy code was created.
Source	Defines the origin of the taxonomy code.

The following section contains step-by-step instructions on how to search for a NCPDP code in the RxConsole application. For additional clarity, each step is accompanied by a corresponding image or screenshot that depicts the action described.

17.1. Search for an NCPDP Taxonomy Code

1. Click on the *NCPDP Taxonomy Code Mapping* button, located on the left-hand side of the screen.

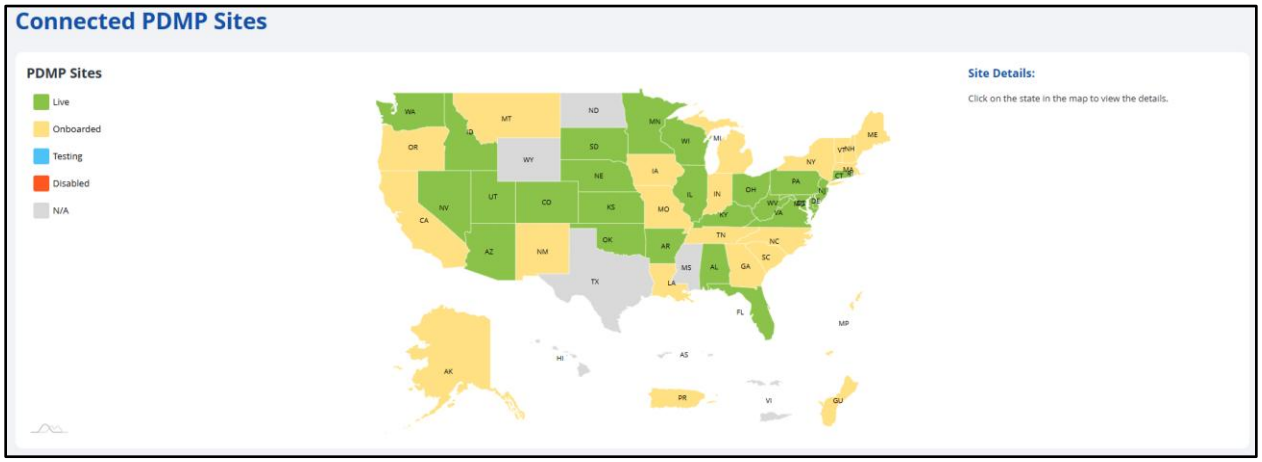


2. Locate the code mapping you are searching for by either:
   a. Scrolling through the list of codes displayed on the screen and sifting through the pages by clicking the arrows under the *Code Mapping* table.
   b. Locate the mapping directly by entering the taxonomy code, description, or PMIX role into the search box labeled, *Filter Mapping* in the top right corner of the screen.

18. System Information

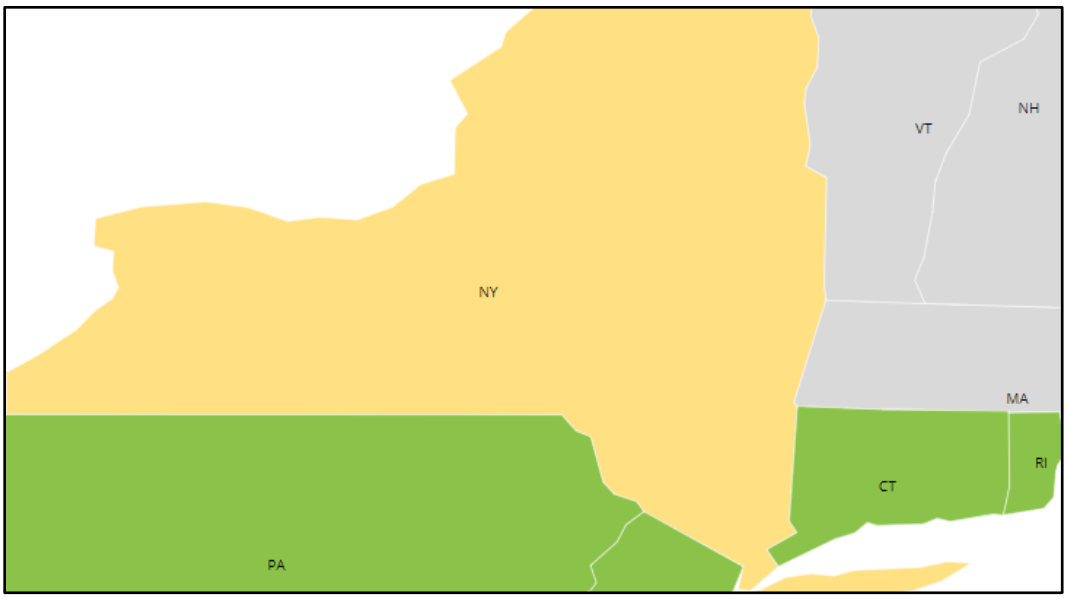
The System Information feature presents a graphical map of the United States, illustrating the deployment and connection status of each state within the RxCheck network.

The screenshot below displays the U.S. map with color-coded indicators representing each state's current integration status with the RxCheck System. The accompanying table provides an explanation for each color code used in the visualization.

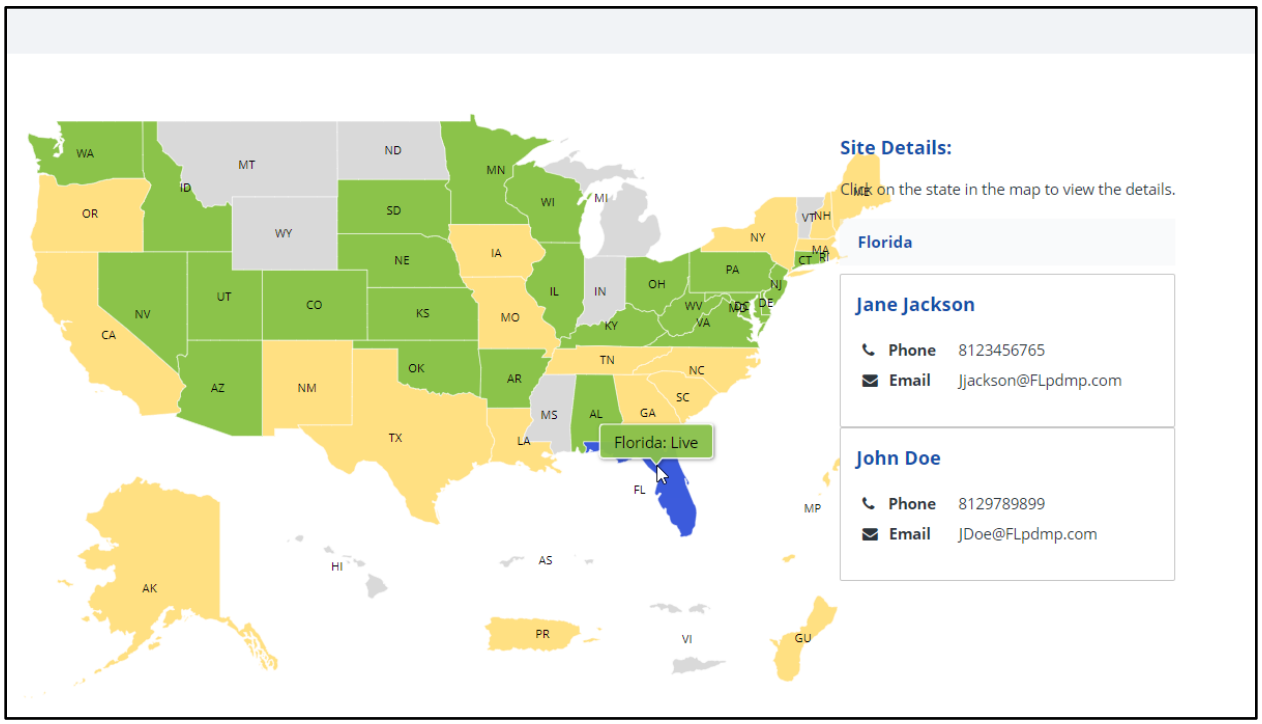


Status	Color Code	Color
Live	Green	
Onboarded	Yellow	
Testing	Blue	
Disabled	Orange	
N/A	Gray	

Users can zoom into any region of the map by double-clicking on the respective area(s). The screenshot below shows a zoomed-in version of New York and Connecticut.



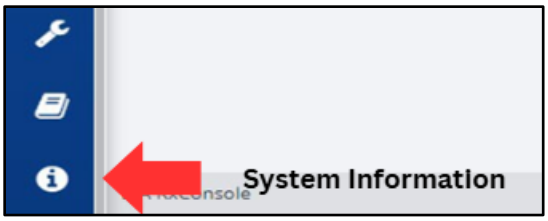
Clicking on each state will also display additional site details, such as the phone and email address of the point-of-contact person for that state, as seen in the diagram below.



The following subsection contains step-by-step instructions on how to view the system information for connected PDMP sites in the RxConsole application. For additional clarity, each step is accompanied by a corresponding image or screenshot that depicts the action described.

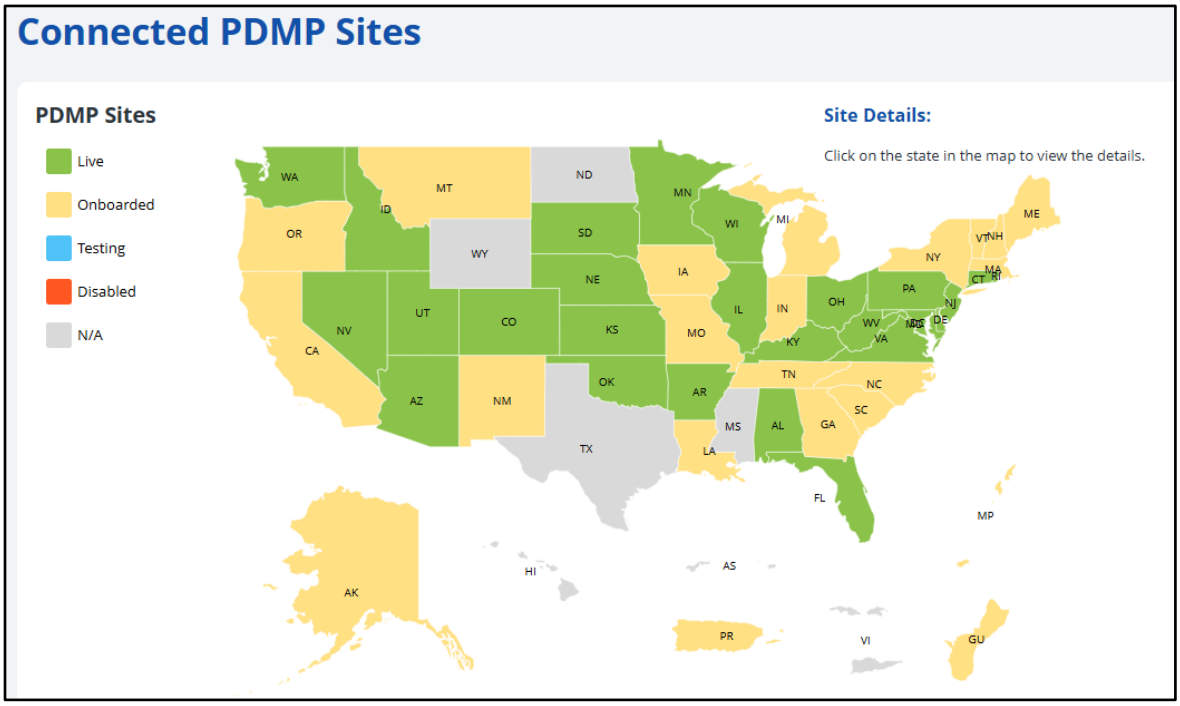
18.1. Connected PDMP Sites

1. Click on the *System Information* button, located on the left-hand side of the screen.



2. A map of *Connected PDMP Sites* is displayed. Proceed to click on a state for additional information or zoom in on a region.

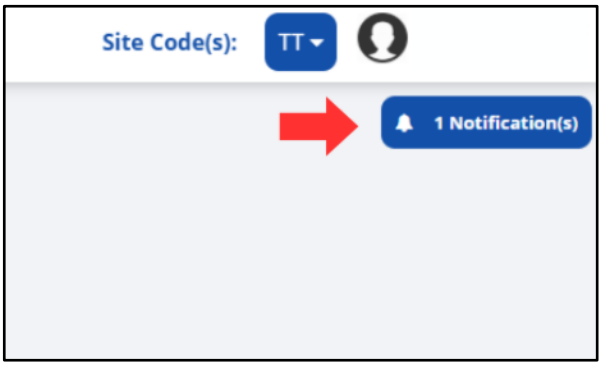
   Notes: See the *System Information* section above for more information.



19. System Notifications

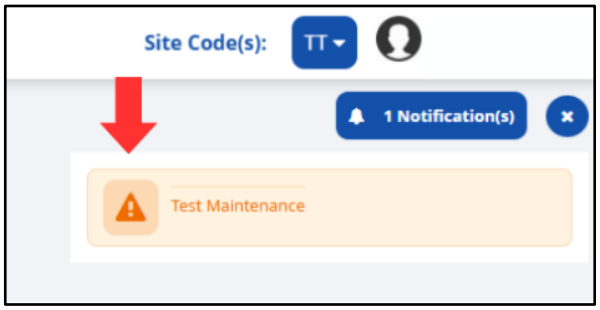
In addition to Heartbeat Notifications, RxConsole offers system notifications within the application. These applications are designed to remind or notify users of important information.

1. After logging into the RxConsole application, a PDMP Administrator will be able to see the *Notification(s)* icon in the top right corner under their name.

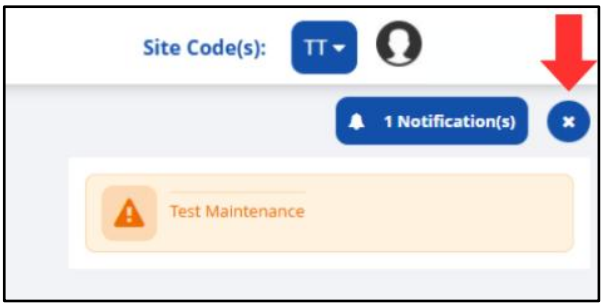


2. Clicking on the *Notification(s)* icon, will display the message relating to the notification, if a notification exists.

   Note: The number of notifications will appear between the "Bell" icon and the word "Notification" on the button.



3. Clicking on the blue circle *X* button will minimize the notification.

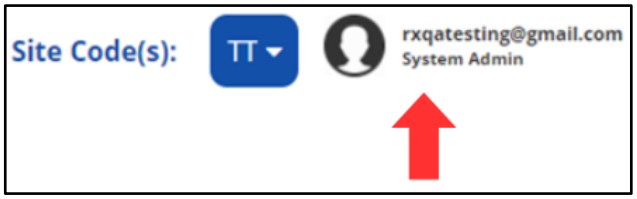


Notifications will be shown for:

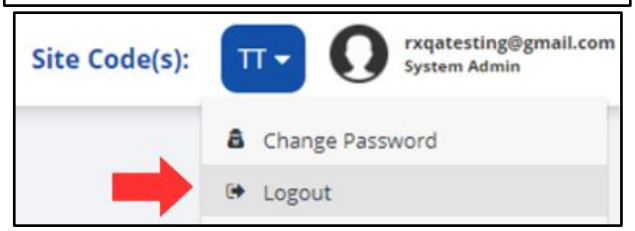
- Heartbeat Notifications
- New MOU Worksheets
- Scheduled Maintenance Events
- Certificate Expirations
- Release Updates

20. Exit the RxConsole application

1. Click on your Username, as displayed on the top right-hand corner of the screen.

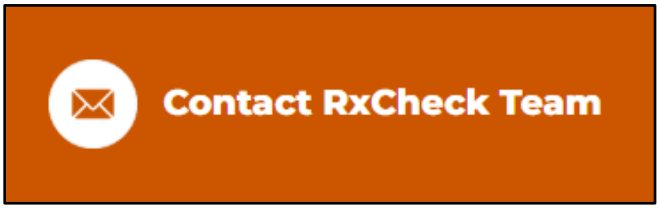


2. Select the *Logout* dropdown option.



21. Contact the RxCheck Team

To connect with the RxCheck team, visit the RxCheck website at www.rx-check.org and click the *Contact RxCheck Team* button located on the orange ribbon near the bottom of the page, or access the contact form directly at www.rx-check.org/ContactUs.



22. Version History Log

Version	Author(s)	Date	Change Log
1.0	IJIS Institute		Initial release
2.0	IJIS Institute	04-2018	
2.1	IJIS Institute	04-2020	
3.0	IJIS Institute	11-2022	
3.1	IJIS Institute	06-2023	
3.1.2	Tetra Ventures	04-2025	

This document will be updated periodically as new functionality is added to the RxCheck hub. If you have any questions or suggestions about the contents of this Guide, please email TTAC at pdmpttac@iir.com.

23. Appendix

This section includes references, citations, and the sources of any additional or supplementary information used in the creation of this guide.

1. https://www.izooto.com/blog/understanding-http-https-protocols
2. https://en.wikipedia.org/wiki/IP_address
3. http://www.healthprovidersdata.com/hipaa/codes/taxonomycodes.aspx
4. http://niem.github.io/health/tutorials/101/
5. https://en.wikipedia.org/wiki/National_Council_for_Prescription_Drug_Programs
6. https://www.hl7.org/implement/standards/