



# RxConsole State PDMP Administrator Guide

Version 3.2

## ***Table of Contents***

<b>1.</b>	<b>Introduction.....</b>	<b>1</b>
1.1.	Purpose of the RxConsole User Guide.....	1
1.2.	Who is the user guide intended for? .....	1
1.3.	RxConsole Access, Registration, and Authorization .....	1
<b>2.</b>	<b>History and Overview of the RxConsole Application .....</b>	<b>2</b>
<b>3.</b>	<b>Functionality of the RxConsole Application.....</b>	<b>3</b>
3.1.	RxConsole Home Page .....	4
3.2.	User Roles and Privileges in the RxConsole Application.....	4
<b>4.</b>	<b>Getting Started With the RxConsole Application.....</b>	<b>7</b>
4.1.	Open the RxConsole Application .....	7
4.2.	Open the RxConsole Test Site (UAT) Application .....	8
4.3.	Sign In to the RxConsole Application .....	8
4.4.	Reset Your Mobile Authenticator App.....	11
4.5.	Retrieve a Forgotten Password.....	13
4.6.	Account Time-Out and Lockout .....	14
4.7.	Reset the Password for Your RxConsole Account.....	15
<b>5.</b>	<b>RxCheck Dashboard .....</b>	<b>16</b>
5.1.	Apply Filters to the RxCheck Dashboard.....	16
5.2.	View Incoming and Outgoing Requests in the RxCheck Dashboard.....	19
5.3.	Graphical Analysis .....	20
<b>6.</b>	<b>Analytical Insights .....</b>	<b>22</b>
6.1.	View Patient and Provider Prescriptions Data in Analytical Insights.....	25
<b>7.</b>	<b>State Routing Service (SRS) Configuration.....</b>	<b>28</b>
7.1.	Site Unique Identifier/Description.....	30
7.2.	SRS Outbound Sender Endpoint .....	31
7.3.	RxCheck Hub Service Host Endpoint.....	35
7.4.	SRS Inbound Sender Endpoint .....	35
7.5.	Site PDMP Application Endpoint.....	37
7.6.	SRS Certificate .....	38
7.7.	Configure the SRS.....	39

7.8.	Configuring the Required Fields.....	40
7.9.	Heartbeat and Health Monitoring .....	41
7.9.1	Current Site Monitoring.....	41
7.9.2.	All Sites Monitoring.....	43
7.10.	Heartbeat Notifications .....	46
<b>8.</b>	<b>Hub Audit Logs.....</b>	<b>48</b>
8.1.	Read the Hub Audit Logs.....	49
8.2.	Filter the Hub Audit Logs .....	51
8.3.	Download the Hub Audit Logs .....	53
8.4.	Exporting the Logs to an sFTP Server.....	54
8.5.	Using an API to Download the Logs.....	56
<b>9.</b>	<b>HCEs .....</b>	<b>57</b>
9.1.	Add a New HCE Site .....	58
9.2.	Breakdown of HCE Site Details .....	60
9.2.1.	Site Details.....	61
9.2.2.	Contact Details.....	62
9.2.3.	Vendor Details .....	63
9.2.4.	Manage Roles .....	64
9.2.5.	Manage Facilities.....	65
9.2.6.	User Administration .....	68
9.3.	Open an HCE Record .....	69
9.4.	Export a List of Your HCEs and Facilities.....	70
<b>10.</b>	<b>Interstate Data Sharing .....</b>	<b>73</b>
10.1.	Select States for Interstate Data Sharing.....	74
10.2.	Deselect States for Interstate Data Sharing.....	75
10.3.	MOU Worksheet(s) .....	77
10.3.1	Populate and Submit the MOU Worksheet .....	77
10.3.2.	Review and Respond to an MOU Worksheet Submitted to Your State .....	79
<b>11.</b>	<b>Interstate Data Sharing—Role Management.....</b>	<b>81</b>
11.1.	Select Roles for Interstate Data Sharing.....	81
11.2.	Deselect Roles for Interstate Data Sharing.....	83

<b>12. Integration Requests.....</b>	<b>85</b>
12.1. Search for Integration Requests .....	86
<b>13. Approving Interstate Data Sharing for HCEs.....</b>	<b>88</b>
13.1. Approve or Revoke Interstate Data Sharing Requests .....	89
<b>14. User Management .....</b>	<b>92</b>
14.1. Search for and Update User Information .....	92
14.2. Adding Users .....	94
14.3. Unlocking a User Account .....	95
<b>15. Provider Validation .....</b>	<b>96</b>
15.1. View and Add a Datasource for Provider Validation .....	96
15.2. View, 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.....	104
15.3.1. Modify an Existing Provider Validation.....	104
15.3.2. Add a New Provider Validation .....	106
<b>16. PDMP Maintenance Schedule .....</b>	<b>109</b>
16.1. Create and Modify a Maintenance Event.....	110
<b>17. NCPDP Taxonomy Code Mapping .....</b>	<b>114</b>
17.1. Search for an NCPDP Taxonomy Code.....	115
<b>18. System Information .....</b>	<b>116</b>
18.1. Connected PDMP Sites .....	118
<b>19. System Notifications .....</b>	<b>119</b>
<b>20. Exit the RxConsole Application.....</b>	<b>120</b>
<b>21. Contact the RxCheck Team .....</b>	<b>121</b>
<b>22. Version History Log .....</b>	<b>122</b>
<b>23. Appendix .....</b>	<b>123</b>



# 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 3.2 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 (HCEs) to connect to their respective PDMPs and offers states a centralized solution for managing these connections. It is 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) to provide a secure, cost-free, and standardized method for interstate sharing of prescription drug data. Funded by BJA, managed by IJIS, and administered by the RxCheck Advisory Body—comprised of PDMP representatives from participating states and territories—RxCheck is the only federally designated, nonproprietary 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 undetected across state lines, 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 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 3.2.

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 SRS 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.



#### **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 data sharing.



#### **Interstate Data Sharing Role Management**

- Manage roles and permissions for interstate data 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 Drug Enforcement Agency (DEA) numbers, National Provider Identifiers (NPI), and state license numbers.



### Maintenance Scheduling

- Create, monitor, and track system maintenance events.



### Taxonomy Code Search

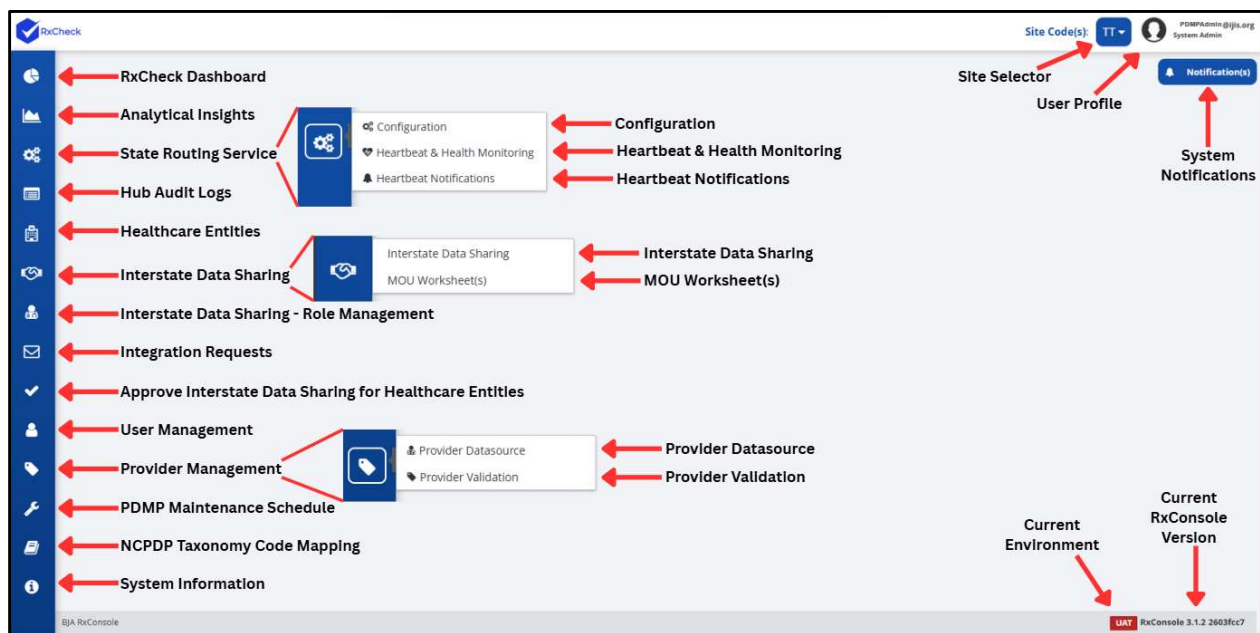
- Search and view mappings related to the National Council for Prescription Drug Programs (NCPDP) Taxonomy Code.



### 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 four main user roles:

- SUPER\_ADMIN \*Only available to the developers of the RxCheck system.
- ADMIN

- VENDOR\_USER
- SUB\_ADMIN
- USER

**Note:** SUPER\_ADMIN information is included for informational purposes only.

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

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

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

RxCheck Console Module	ADMIN- State	ADMIN- Vendor	VENDOR_ USER	SUB_ADMIN	USER
<b>RxCheck Dashboard</b>	X	X	-	-	-
<b>Analytical Insights</b>	X	-	-	-	-
<b>State Routing Service</b>	X	X	X	X	-
<b>Hub Audit Logs</b>	X	X	X	X	X
<b>Healthcare Entities</b>	X	X (view only)	X (view only)	-	-
<b>Interstate Data Sharing</b>	X	X	-	-	-
<b>Interstate Data Sharing—Role Management</b>	X	X	-	-	-
<b>Integration Requests</b>	X	-	-	-	-
<b>Approve Interstate Data Sharing for Healthcare Entities</b>	X	-	-	-	-
<b>User Management</b>	X	-	-	-	-
<b>Provider Management</b>	X	-	-	-	-
<b>PDMP Maintenance Schedule</b>	X	X	-	-	-
<b>NCPDP Taxonomy Code Mapping</b>	X	X	X	X	X
<b>System Information</b>	X	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 HCEs
- 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 on two distinct environments: **Production** and **Test (UAT)**.

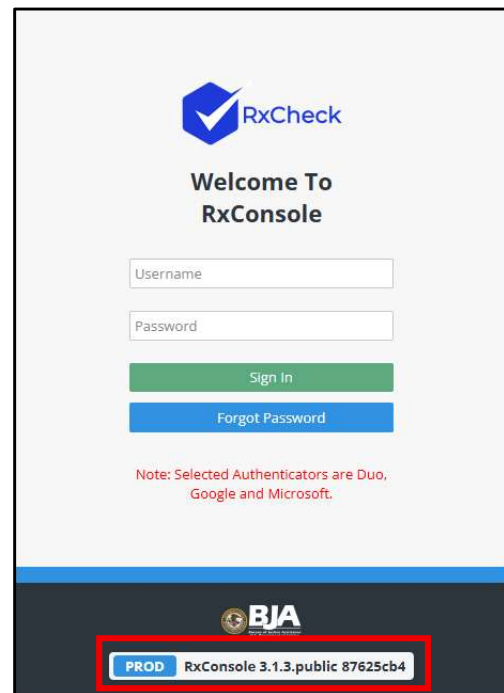
Access to each environment is determined by the specific URL used. The URL will indicate if you are connected to the test or production site, and the login page displays the current application version at the bottom right of the page.

### 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.



RxCheck

Welcome To  
RxConsole

Username

Password

Sign In

Forgot Password

Note: Selected Authenticators are Duo, Google and Microsoft.

BJA

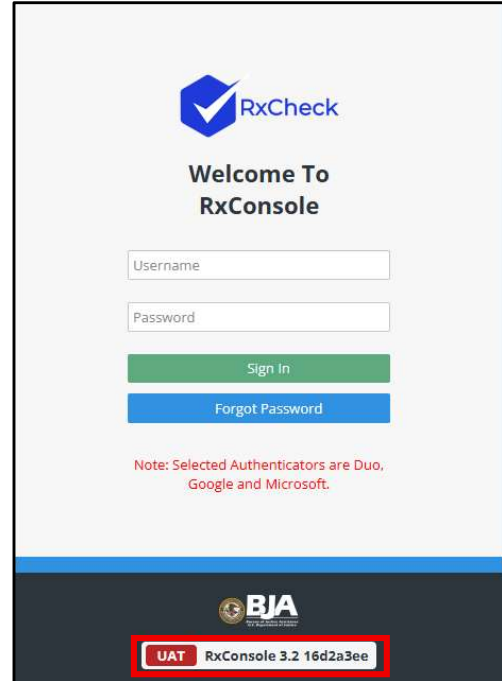
PROD RxConsole 3.1.3.public 87625cb4

## 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 that the site type is Test “(UAT),” along with the RxConsole version number.



## 4.3. Sign In to the RxConsole Application

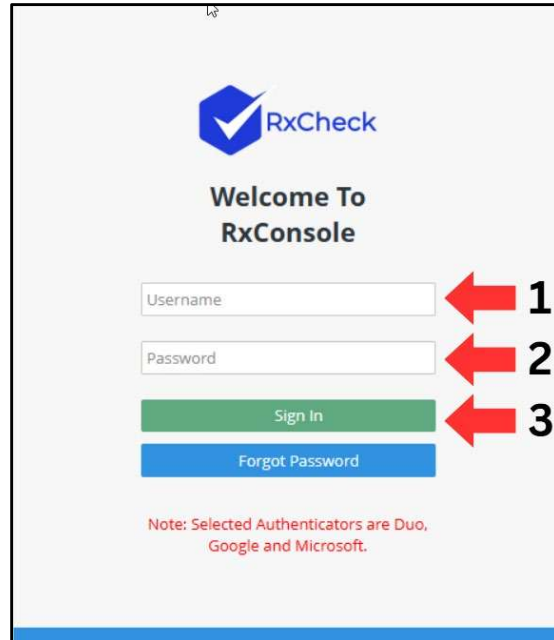
Personal login credentials are required to log into the RxConsole application. Login credentials will be provided to the state PDMP administrators during the onboarding process. **For further inquiries regarding your login credentials, please contact the RxCheck help desk, as described in the [Contact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



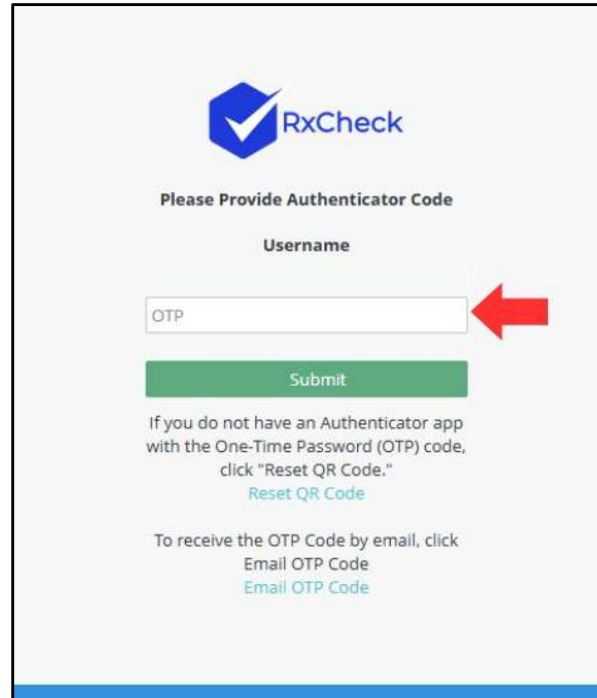
The image shows the RxCheck login interface. At the top is the RxCheck logo. Below it is the text "Welcome To RxConsole". There are two input fields: "Username" and "Password". Below these are two buttons: "Sign In" (green) and "Forgot Password" (blue). Red arrows with numbers 1, 2, and 3 point to the Username field, Password field, and Sign In button respectively. At the bottom, there is a note: "Note: Selected Authenticators are Duo, Google and Microsoft."

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)

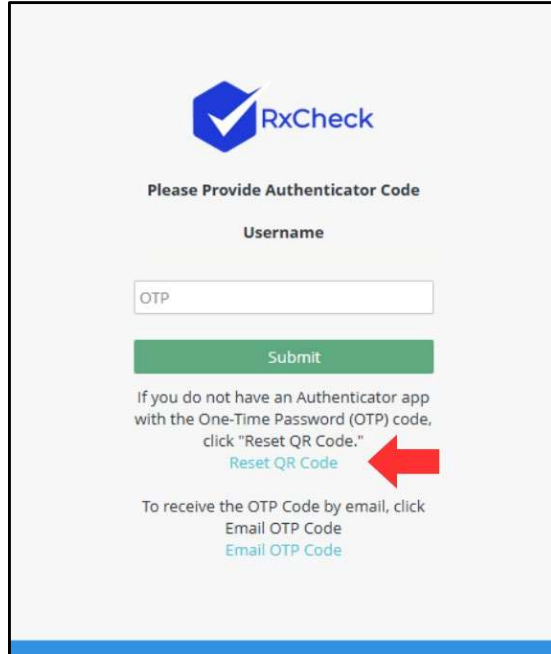
6. Enter the OTP code from the email or authenticator app and click on the *Submit* button.



The image shows a login page for RxCheck. At the top is the RxCheck logo, which consists of a blue hexagon with a white checkmark inside, followed by the text "RxCheck". Below the logo is the heading "Please Provide Authenticator Code". Underneath this is the label "Username". There is a text input field with the placeholder text "OTP". A red arrow points to the right side of this input field. Below the input field is a green button with the text "Submit". Below the button, there is a paragraph of text: "If you do not have an Authenticator app with the One-Time Password (OTP) code, click 'Reset QR Code.'" followed by a blue link "Reset QR Code". At the bottom, there is another paragraph: "To receive the OTP Code by email, click Email OTP Code" followed by a blue link "Email OTP Code". The entire page has a light gray background and a blue footer bar at the bottom.

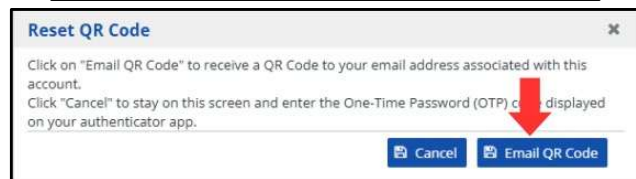
## 4.4. Reset Your Mobile Authenticator App

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



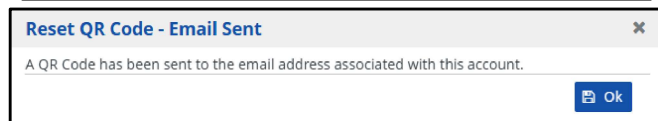
The screenshot shows the RxCheck login page. At the top is the RxCheck logo. Below it, the text 'Please Provide Authenticator Code' is displayed. Underneath is a 'Username' label and an input field labeled 'OTP'. A green 'Submit' button is below the input field. Below the button, there is instructional text: 'If you do not have an Authenticator app with the One-Time Password (OTP) code, click "Reset QR Code."'. A red arrow points to the 'Reset QR Code' link. Below this, another line of text says 'To receive the OTP Code by email, click Email OTP Code', with a link 'Email OTP Code' below it.

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



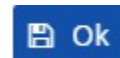
The screenshot shows a dialog box titled 'Reset QR Code'. It contains the following text: 'Click on "Email QR Code" to receive a QR Code to your email address associated with this account.' and 'Click "Cancel" to stay on this screen and enter the One-Time Password (OTP) code displayed on your authenticator app.' At the bottom right, there are two buttons: 'Cancel' and 'Email QR Code'. A red arrow points to the 'Email QR Code' button.

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

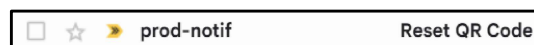


The screenshot shows a pop-up window titled 'Reset QR Code - Email Sent'. It contains the text: 'A QR Code has been sent to the email address associated with this account.' At the bottom right, there is an 'Ok' button.

4. Press the *Ok* button.



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



The screenshot shows the header of an email notification. It includes a checkbox, a star icon, a right-pointing arrow, the text 'prod-notif', and the subject 'Reset QR Code'.

6. Open the email and scan the QR code.

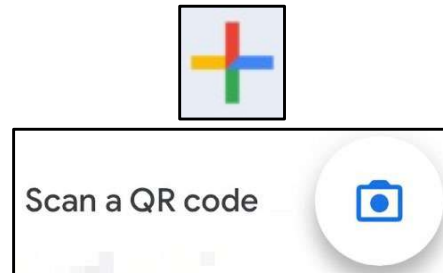
**Note:** The QR code here is for reference only.



**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.

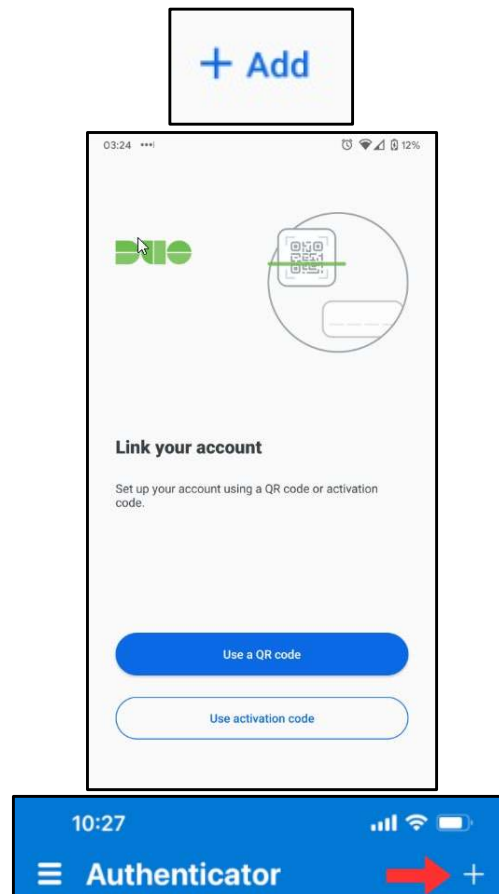
### Set Up Using the Google Authenticator App

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 the Duo Mobile Authenticator App

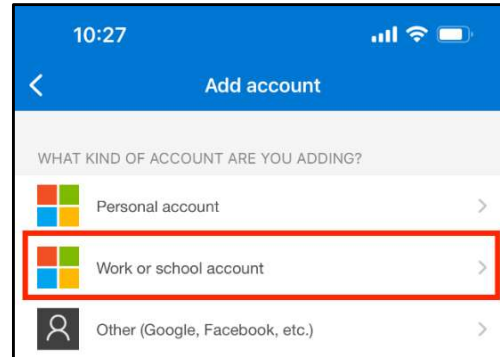
1. Launch the Duo Mobile Authenticator app on your mobile device.
2. Press the + Add button.
3. Press the **Use QR Code** button.
4. Scan the QR code in the RxConsole email.



### Set Up Using the Microsoft Authenticator App

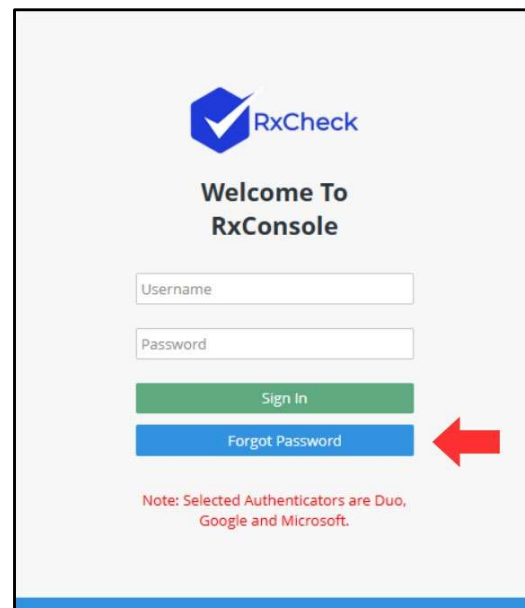
1. Launch the Microsoft Authenticator app on your mobile device.
2. Press the + icon.
3. Select *Work or School Account*.
4. Press the *Scan QR Code* option.

5. Scan the QR code in the RxConsole email.

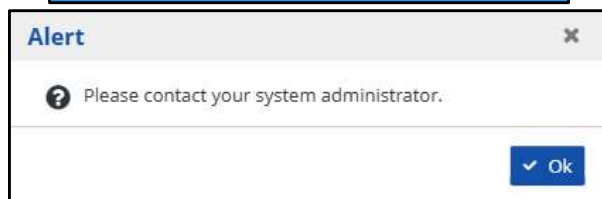


#### 4.5. Retrieve a Forgotten Password

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 that they use to log into the RxConsole application** to the RxConsole support team.

## 4.6. Account Time-Out and Lockout

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

**Time-Out**—All RxConsole roles will experience a 15-minute period in which they will not be able to access the RxConsole application after five failed password attempts. After the 15-minute time-out 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.

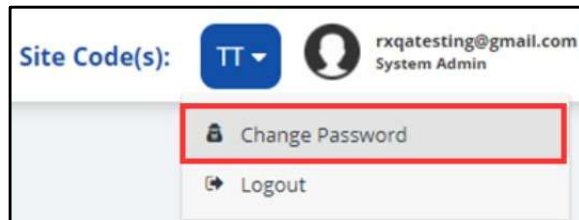
## 4.7. Reset the Password for Your RxConsole Account

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.

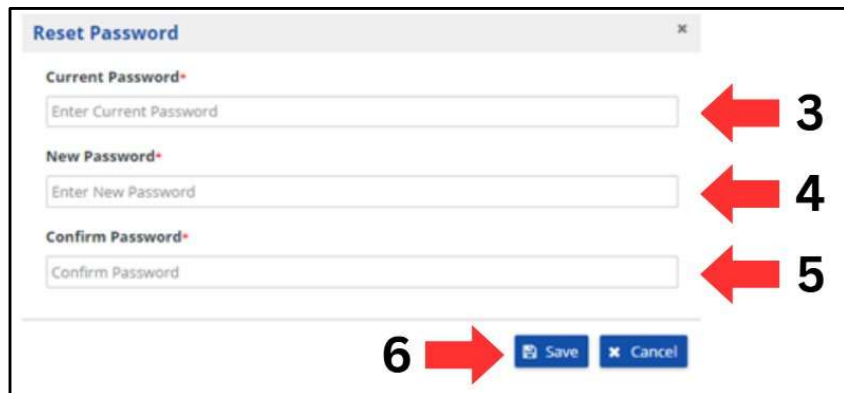
1. Click on your username on the top-right corner of the screen.



2. Select the *Change Password* drop-down 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.

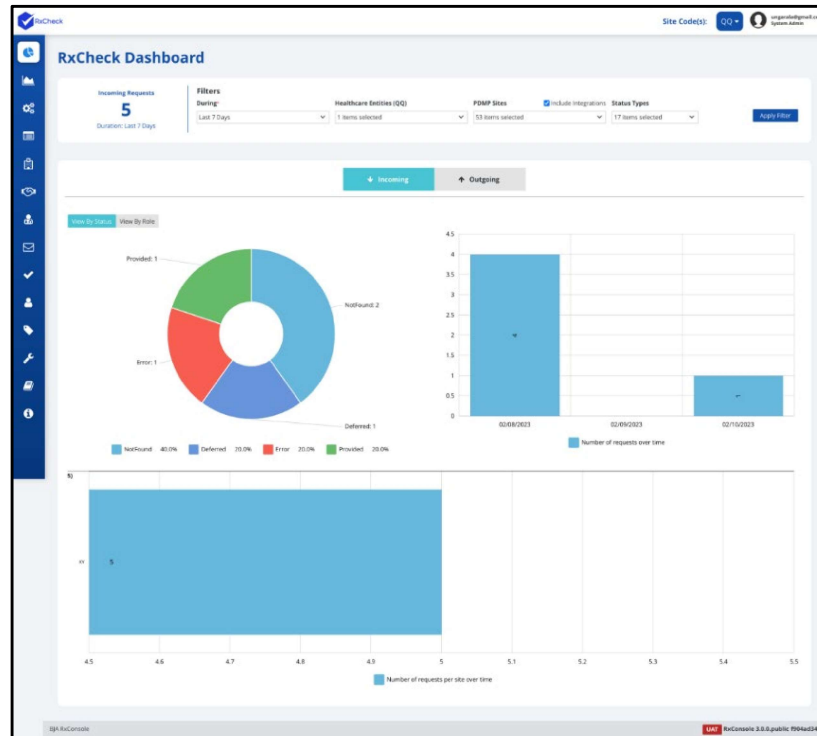


**Note:** This ensures that the user enters the new password as intended.

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

## 5. RxCheck Dashboard

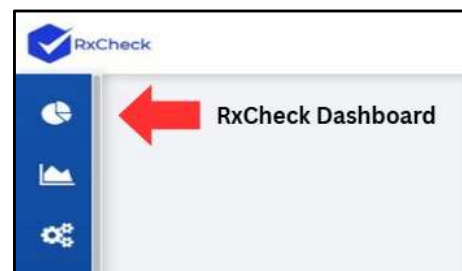
The RxCheck Dashboard provides a location for PDMP administrators and other authorized users to view metrics on their state's RxCheck usage.



**Note:** The RxCheck Dashboard will only work after the PDMP SRS is configured. Information regarding the SRS, 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

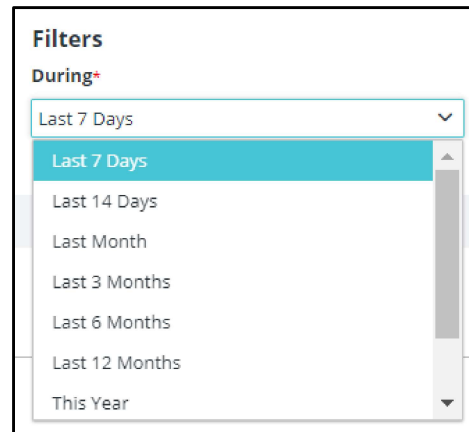
1. Click the pie graph icon on the left-hand side of the screen to access the RxCheck Dashboard.
2. Click on the downward-facing arrow for the filter titled "During" to reveal options to filter by.





3. Select the period to match the historical time frame that you would like to populate the RxCheck Dashboard.

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



**Filters**

**During\***

- Last 7 Days
- Last 14 Days
- Last Month
- Last 3 Months
- Last 6 Months
- Last 12 Months
- This Year

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

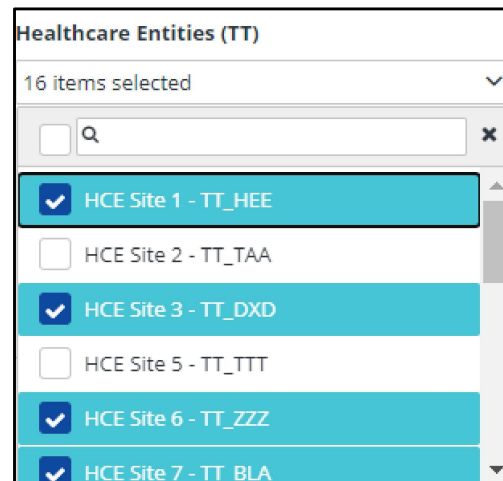


**Healthcare Entities (TT)**

13 items selected

5. Select the desired HCEs by:
  - a. Scrolling through the drop-down and checking the box next to each desired entity.
  - 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.



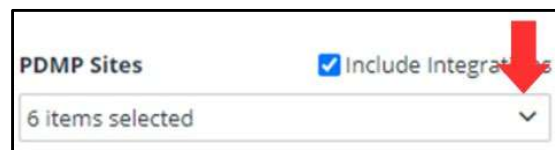
**Healthcare Entities (TT)**

16 items selected

☐

- ☒ HCE Site 1 - TT\_HEE
- ☐ HCE Site 2 - TT\_TAA
- ☒ HCE Site 3 - TT\_DXD
- ☐ HCE Site 5 - TT\_TTT
- ☒ HCE Site 6 - TT\_ZZZ
- ☒ HCE Site 7 - TT\_BLA

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



**PDMP Sites**

☒ Include Integrations

6 items selected

7. Select the desired PDMP site(s) by:
  - a. Scrolling through the drop-down and checking the box next to each desired state.
  - 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 HCEs.

**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 drop-down and checking the box next to each desired status.
  - b. Typing in the **Search Bar** to filter the status types.

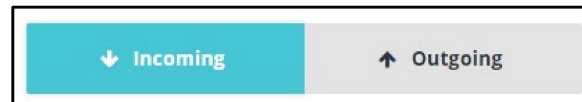
**Note:** By default, all options are selected. To clear your selections, click the checkbox next to the search bar before choosing your desired options.

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

Apply Filter

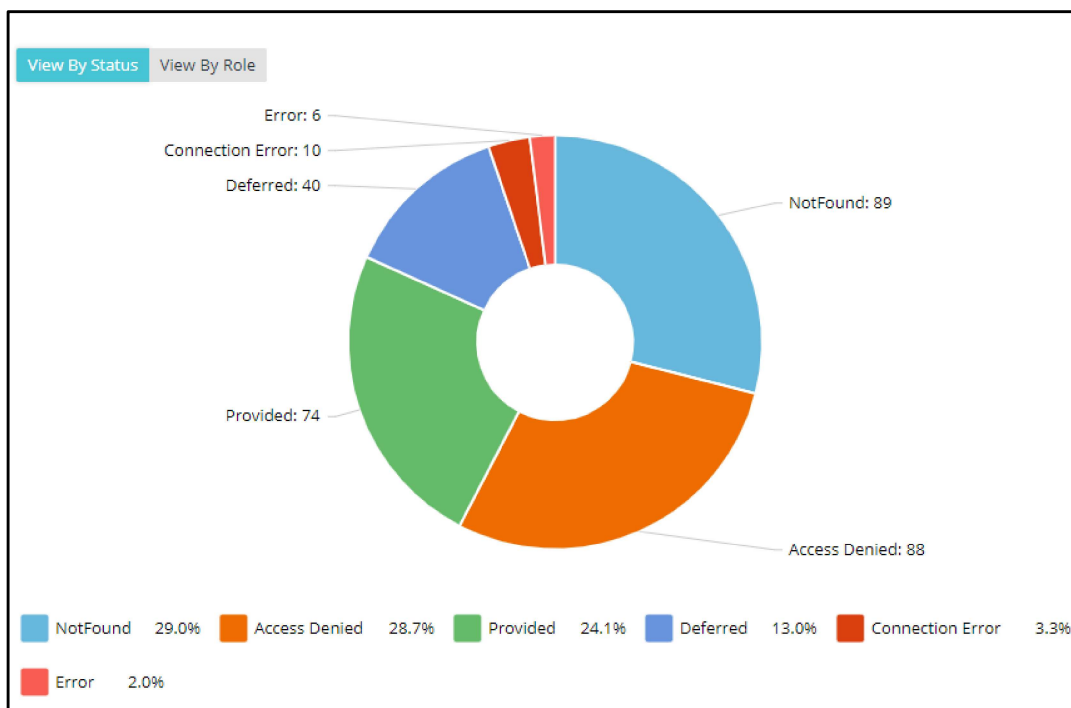
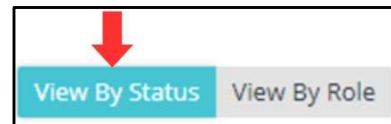
## 5.2. View Incoming and Outgoing Requests in the RxCheck Dashboard

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.

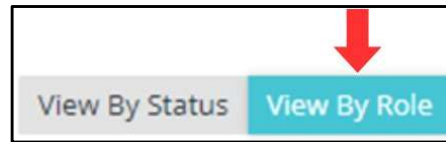


**Note:** The *Incoming* option is selected and displayed by default.

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.



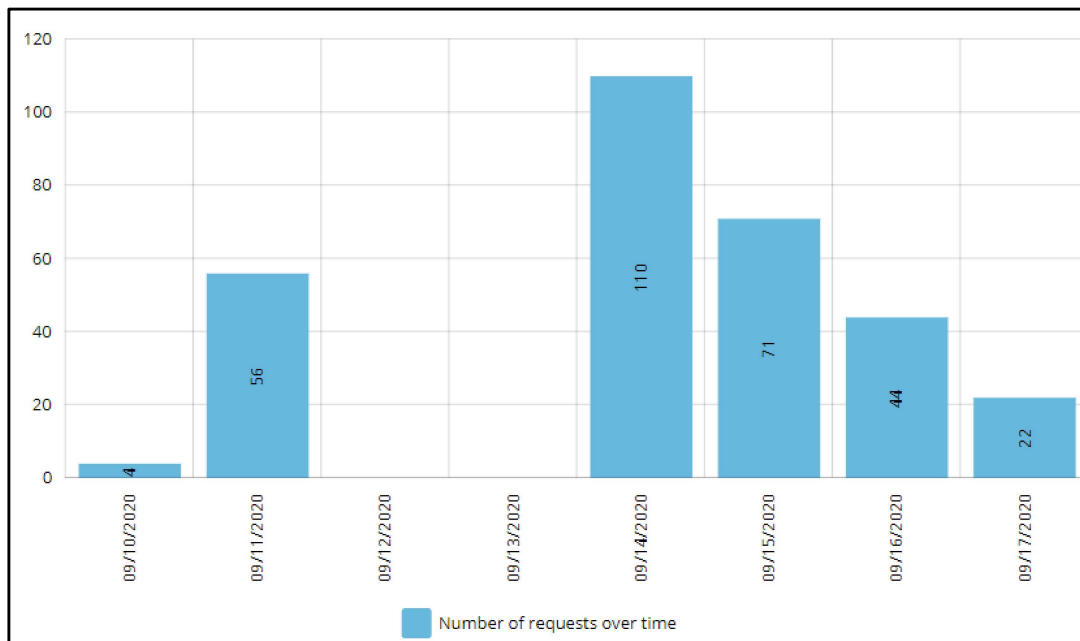
View By Status View By Role	
Role Name	Count
Psychologists	16
PhysiciansX	4
Physicians	287

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

### 5.3. Graphical Analysis

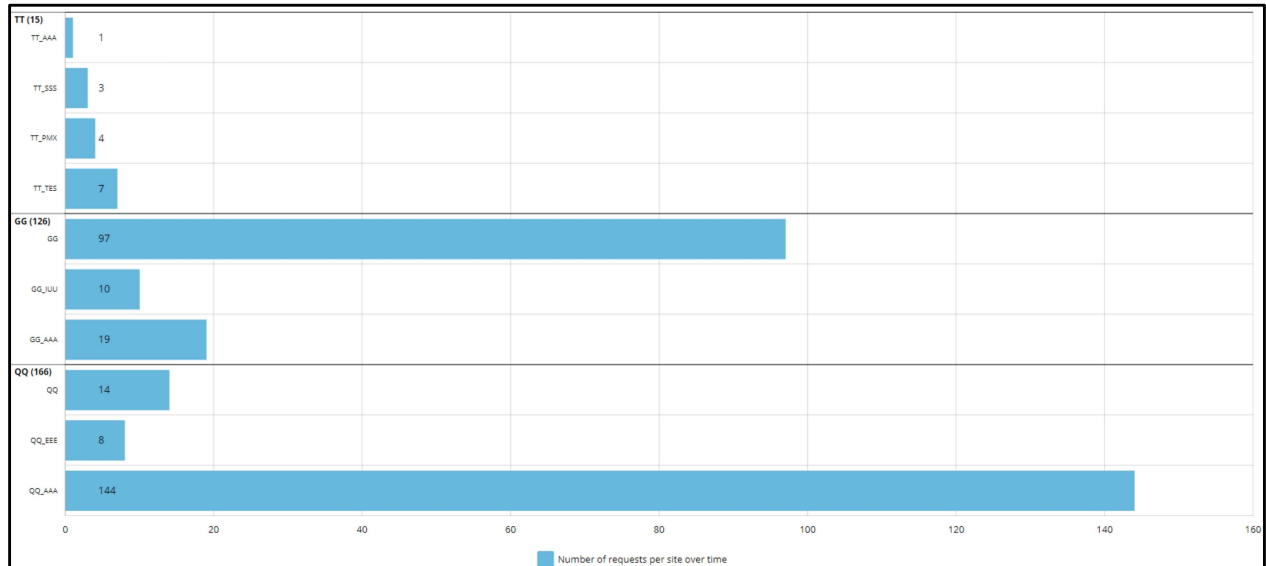
The following bar graph depicts the distribution of requests over time, matching your selected dashboard filters.

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 sites 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

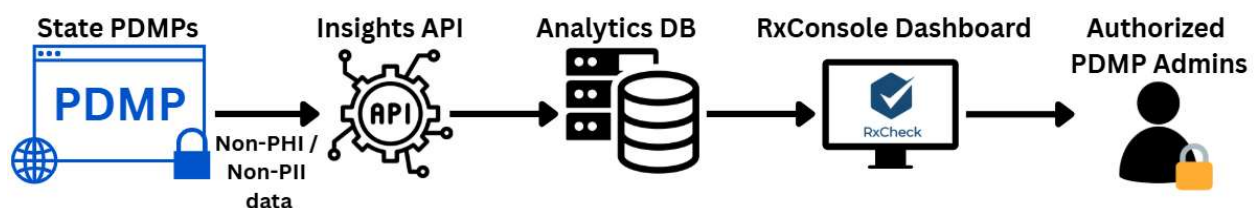
The Analytical Insights dashboard allows each state to analyze prescription trends and patterns at a high level. It provides visibility into how prescriptions from other states are being dispensed within the state, as well as how the state's own prescriptions are being filled outside its borders. This 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 protected health information (PHI) or personally identifiable information (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 Application Programming Interface (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 in 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 the RxConsole.

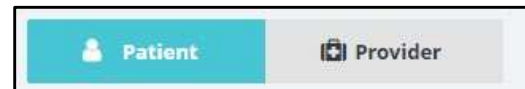


## 6.1. View Patient and Provider Prescriptions Data in Analytical Insights

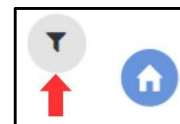
1. Click the area graph icon on the left-hand side of the screen to access the RxCheck Dashboard.



2. Click on the *Patient* or *Provider* button located in the top middle of the page, depending on the information that 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.

A screenshot of the search filters panel. It includes a 'Request Type' section with 'Incoming' and 'Outgoing' buttons, a 'Time Range' dropdown set to 'Last Month', a 'Search by' section with 'County' and 'Zip Code' radio buttons, and a 'County' dropdown set to 'Choose'. At the bottom are 'Search' and 'Reset Filters' buttons.

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

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

A close-up of the 'Request Type' section. It shows two buttons: 'Incoming' (highlighted in teal with a downward arrow) and 'Outgoing' (grey with an upward arrow).

6. Use the *Time Range* drop-down to select a period that you want to display.

A screenshot of the 'Time Range' dropdown menu. The menu is open, showing options: 'Last Month' (highlighted in teal), 'Last 3 Months', 'Last 6 Months', 'Last 12 Months', and 'Custom Date Range'.

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

Search by  
☒ County ☐ Zip Code

### How to Search by County

1. Click on the *County* radio button.

Search by  
☒ County ☐ Zip Code

**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.

County:  
Choose ▼

3. Select your county by:
- Scrolling through the drop-down options and checking the box.
  - Typing in the search bar to filter results.

County:  
Choose ▼

☐ Atlantic  
☐ Bergen  
☐ Burlington  
☐ Camden  
☐ Cape May  
☐ Cumberland

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

Search

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.



Search by

☐ County ☒ Zip Code

A red arrow points down to the 'Zip Code' radio button.

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



Zip Code Range:

Zip Code:  miles  mi.

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

 Search

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.

 Reset Filters

## 7. State Routing Service (SRS) Configuration

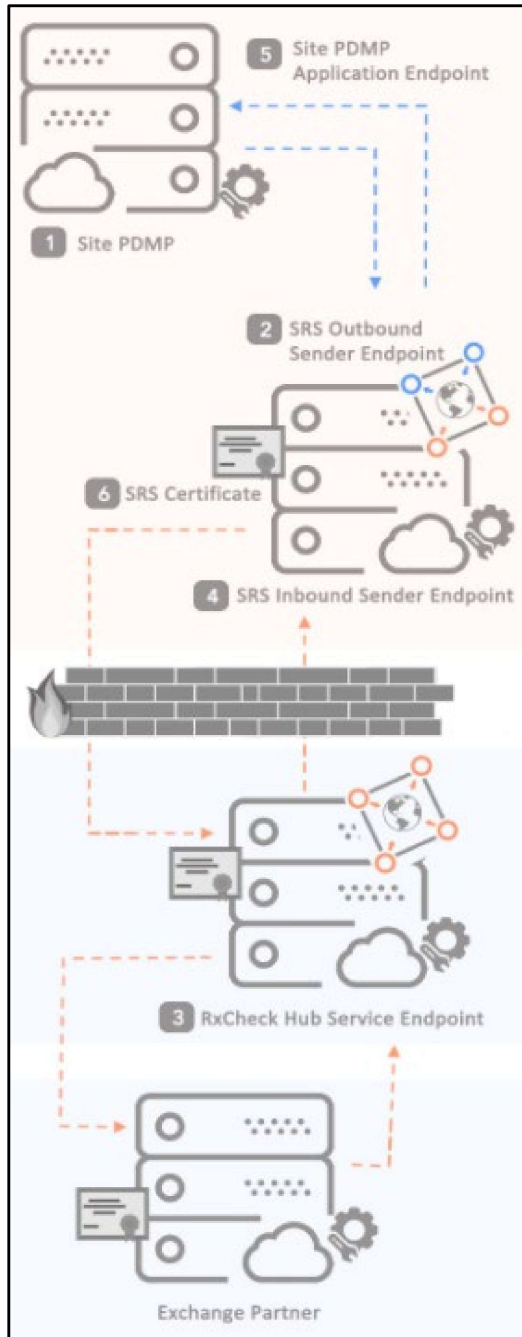
Every state PDMP officially onboarded into the RxCheck system will have a routing service installed that allows it to send and receive messages from other states. Message content between states is encrypted for privacy and security purposes and can only be accessed and decrypted by the state intended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

The screenshot displays the 'State Routing Service Configuration' page within the RxCheck application. On the left, a diagram illustrates the SRS architecture, showing the flow from a 'Site PDMP' through an 'SRS Outbound Sender Endpoint' to an 'RxCheck Hub Service Endpoint', and from an 'RxCheck Hub Service Endpoint' through an 'SRS Inbound Sender Endpoint' back to the 'Site PDMP'. The main configuration area on the right contains a list of fields for setting up the SRS, each with a plus icon and a dropdown menu:

- 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

At the bottom right of the configuration area are 'Save' and 'Cancel' buttons. The top right corner shows the 'Site Code: UT' and 'System Admin' user information. The bottom of the interface includes the 'BJA RxConsole' logo and version information: 'UAT RxConsole 3.0.0.public bd37846'.

**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 SRS. The SRS is a software that facilitates the successful transmission of messages between HCEs 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 SRS, the state PDMP admin will need to enter the requested information into the data fields present under each section of the SRS 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 SRS 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.

The screenshot shows a web form titled "State Routing Service Configuration" with a "Save" button in the top right. Below the title is a tab labeled "Site Unique Identifier / Description". The form contains four input fields: "Name" with the value "TT", "Type" with the value "PDMP", "Description" with the value "Test Site TT", and "API key" with a long alphanumeric string: "FLc577a505-a43f-4896-b88e-8c4e76d9e5a21525969705649".

Data Field Name	Description
<b>Name</b>	The official two-letter state abbreviation code assigned to each state. e.g., New Jersey: NJ, California: CA <b><i>This field is auto-populated.</i></b>
<b>Type</b>	The site type assigned to each state is PDMP (Prescription Drug Monitoring Program). <b><i>This field is auto-populated.</i></b>
<b>Description</b>	A brief description of the site. <b><i>This field is auto-populated.</i></b>
<b>API Key</b>	An 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. <b><i>This field is auto-populated.</i></b>

## 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 (NIEM)
- NCPDP 2017: National Council for Prescription Drug Programs (NCPDP)
- HL7 FHIR: Health Level Seven International (HL7) Fast Healthcare Interoperability Resources (FHIR)
- HTML5: Hypertext Markup Language 5 (HTML5)

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

- **PMIX:** The PMIX Standards Organization supports the sharing of 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; enabling secure, trusted exchanges of PDMP data; and promoting 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 interrelated public and private service domains (e.g., law enforcement, public safety, healthcare). 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, multistakeholder 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 and 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.

The screenshot shows a web form titled "2 SRS Outbound Sender Endpoint". The form contains several sections for configuring outbound endpoints:

- Protocol:** A dropdown menu set to "HTTP".
- Port Number:** A text field containing "9080".
- Domain:** A text field labeled "Domain Name".
- IP Address:** A text field labeled "IP Address" with a red border and a red error message "IP Address is required" below it.
- NIEM:** A section with the NIEM logo and a text field for the "PMIX Outbound URL" containing "http://9080/outbound/service".
- NCPDP-2017:** A section with the NCPDP 2017 logo and a text field for the "NCPDP-2017 Outbound URL" containing "http://9080/rxoutbound/webapi/ncdp/2017".
- HL7 FHIR:** A section with the HL7 FHIR logo and a text field for the "FHIR Outbound URL" containing "http://9080/rxoutbound/fhir".
- HTML:** A section with the HTML logo and a text field for the "HTML Outbound URL" containing "http://9080/rxoutbound/report/html".
- Security Credentials:** A section titled "Security Credentials : (HTTP Basic Authentication)" containing two text fields: "Outbound Username" and "Outbound Password".



Heading	Data Field Name	Description
	<b>Protocol</b>	<p>Protocols define a standardized set of rules for formatting and handling data during transmission.</p> <p>State PDMP administrators must select one of the following options from the drop-down menu:</p> <ul style="list-style-type: none"> <li>• <b>HTTP (HyperText Transfer Protocol)</b>—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.</li> <li>• <b>HTTPS (HyperText Transfer Protocol Secure)</b>—An enhanced version of HTTP that uses encryption and authentication mechanisms. HTTPS ensures secure communication by leveraging Secure Socket Layer or Transport Layer Security and is the recommended protocol for transmitting PDMP data within the RxCheck infrastructure.</li> </ul>
	<b>Domain</b>	<p>The domain name of the server on which the SRS is running.</p> <p>This field is <u>optional</u>. If no domain is specified, the system will use the IP address.</p> <p>e.g., New Jersey: NJ.gov</p>
	<b>Port Number</b>	<p>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.</p>
	<b>IP Address</b>	<p>An Internet Protocol (IP) address is a unique numerical identifier assigned to each device that is connected to a network that uses the IP for communication. The IP address field is populated as “localhost” by default.</p>

Heading	Data Field Name	Description
<b>NIEM</b>	<b>PMIX Outbound URL</b>	A fully qualified URL for the NIEM service on outbound SRS. <i>This field is auto-populated.</i>
<b>NCPDP-2017</b>	<b>NCPDP-2017 Outbound URL</b>	A fully qualified URL for the NCPDP 2017 service on outbound SRS. <i>This field is auto-populated.</i>
<b>HL7 FHIR</b>	<b>FHIR Outbound URL</b>	A fully qualified URL for the FHIR service on outbound SRS. <i>This field is auto-populated.</i>
<b>HTML</b>	<b>HTML Outbound URL</b>	A fully qualified URL for the HTML service on outbound SRS. <i>This field is auto-populated.</i>
<b>Security Credentials: (HTTP Basic Authentication)</b>	<b>Outbound Username</b>	A username to authenticate the SRS connection on the RxCheck network.
	<b>Outbound Password</b>	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 PDMP data with other states and integration partners (e.g., HIE and 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 detailed descriptions for each data field presented.

The screenshot displays the 'RxCheck Hub Service Host Endpoint' configuration page. It contains the following fields:

- Protocol:** A dropdown menu set to 'HTTPS'.
- Domain:** A text input field containing 'uat.rxcheck.org'.
- Port Number:** A text input field containing '18803'.
- IP Address:** A text input field containing 'IP Address'.
- PMIX2 Hub Endpoint URL:** A text input field containing 'https://uat.rxcheck.org:18803/RxCheck/pmix2'.

Data Field Name	Description
<b>Protocol</b>	This value cannot be changed and is set to “HTTPS.”
<b>Domain</b>	This value cannot be changed and is automatically set to the hub domain name.
<b>Port Number</b>	This value cannot be changed and is automatically set to the port on which the hub is running.
<b>IP Address</b>	This value cannot be changed and is automatically set to the IP address for the hub.
<b>PMIX2 Hub Endpoint URL</b>	<b><i>This field is auto-populated.</i></b> 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.

The screenshot shows the configuration interface for the SRS Inbound Sender Endpoint. The interface is divided into several sections:

- Protocol:** A dropdown menu set to "HTTPS".
- Domain:** A text input field labeled "Domain Name".
- Port Number:** A text input field containing "8443".
- IP Address:** A text input field containing "10.1.0.8".
- PMIX2 Inbound URL:** A text input field labeled "URL Path".
- IEPD:** A text input field containing "PMIX1".
- Rate Limiting:**
  - Rate Limit:** A text input field containing "0".
  - Time Unit:** A dropdown menu labeled "Select Time Unit".
- Enable Loopback:** A checkbox labeled "Enable Loopback (Same Site Outbound can call same site Inbound)".
- Security Credentials:**
  - Inbound Username:** A text input field labeled "Inbound Username".
  - Inbound Password:** A text input field labeled "Inbound Password".

Heading	Data Field Name	Description
	<b>Protocol</b>	This value can be set to "HTTP" or "HTTPS."
	<b>Domain</b>	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.
	<b>Port Number</b>	Port number where the inbound service is configured.
	<b>IP Address</b>	IP address where the inbound SRS is hosted.
	<b>PMIX2 Inbound URL</b>	<b><i>This field is auto-populated</i></b> 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.
	<b>IEPD</b>	<b><i>This field is auto-populated</i></b> based on the IEPD option selected by the 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.
<b>Rate Limiting</b>	<b>Rate Limit</b>	If a value is entered for this field, it indicates the number of requests to the inbound, with respect to the defined time unit.
<b>Rate Limiting</b>	<b>Time Unit</b>	Defines the unit for the value entered in the <i>Rate Limit</i> field. Can be set to second, minute, hour, day, or month.

Heading	Data Field Name	Description
<b>Enable Loopback (Same Site Outbound Can Call Same Site Inbound)</b>	<b>Enable Loopback</b>	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.
<b>Security Credentials (HTTP Basic Authentication)</b>	<b>Inbound Username</b>	A username to authenticate the SRS connection in the RxCheck network.
	<b>Inbound Password</b>	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.

The screenshot shows a configuration form titled "Site PDMP Application Endpoint". It contains the following fields:

- Protocol**: A dropdown menu with "HTTP" selected.
- Domain**: A text input field labeled "Domain Name".
- Port Number**: A text input field with "9085" entered.
- IP Address**: A text input field with "localhost" entered.
- URL Path**: A text input field with "/rxcheck/pdmp" entered.
- PDMP URL**: A text input field with "http://localhost:9085/rxcheck/pdmp" entered.
- Security Credentials : (HTTP Basic Authentication)**: A section containing two text input fields: "PDMP Username" and "PDMP Password".

Heading	Data Field Name	Description
	<b>Protocol</b>	This value can be set to "HTTP" or "HTTPS."
	<b>Domain</b>	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.
	<b>Port Number</b>	Port number where the website is hosted.

Heading	Data Field Name	Description
	<b>IP Address</b>	IP address of the state PDMP server where the website is hosted.
	<b>URL Path</b>	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 the Super Administrator at the time of PDMP site creation.
	<b>PDMP URL</b>	<i><b>This field is auto-populated</b></i> based on the values selected/entered in protocol, domain/IP address, and port number.
<b>Security Credentials (HTTP Basic Authentication)</b>	<b>Inbound Username</b>	A username, which is an optional parameter that enables basic authentication on the PDMP site.
	<b>Inbound Password</b>	A password, which is an optional parameter that enables basic authentication on the 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
<b>Private Key Subject</b>	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.
<b>Public Key (DER Format)</b>	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.
<b>Certificate Expiry Date</b>	The date when the uploaded certificate expires.

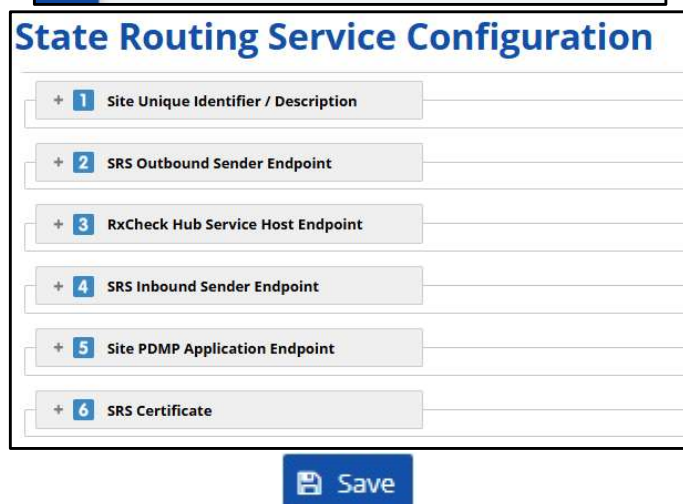
## 7.7. Configure the SRS

Once the previous sections have been populated on the SRS Configuration page, the state PDMP administrator can save the details and complete the configuration process.

1. Click on the *SRS 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.

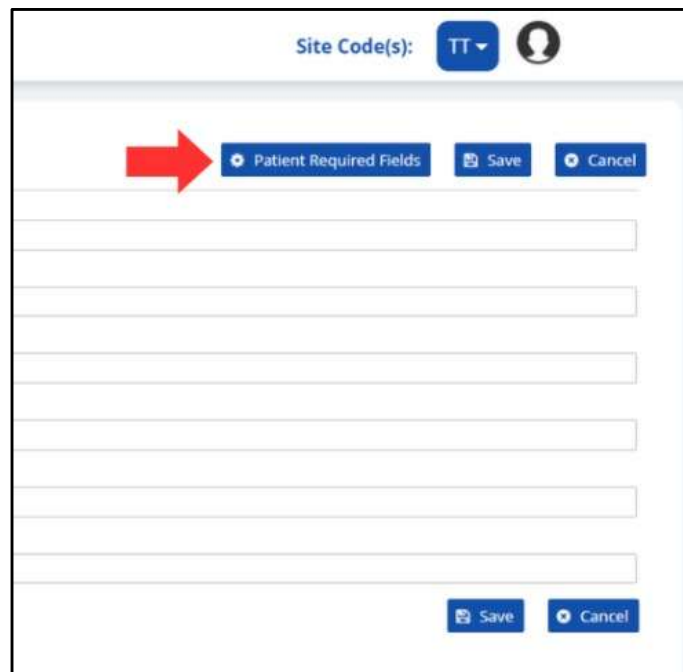


3. Click the *Save* button.

## 7.8. Configuring the Required Fields

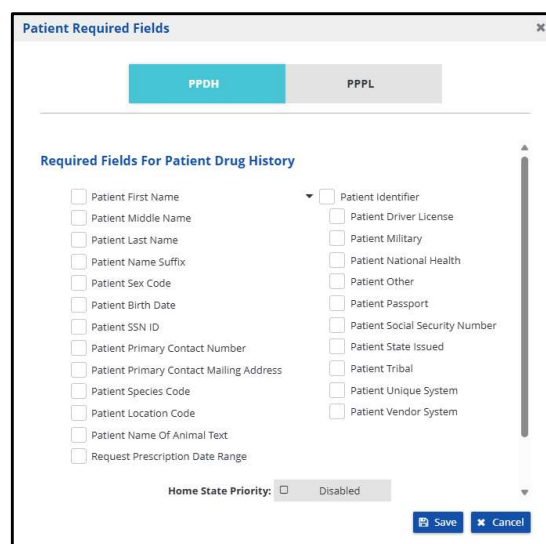
Each state PDMP administrator can configure the PMIX fields required in the request message to search for a patient in the PDMP system. The name-matching algorithm implemented within the PDMP system determines these required fields.

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



The screenshot shows a web interface for SRS configuration. At the top, there is a 'Site Code(s):' dropdown menu set to 'TT' and a user profile icon. Below this, a red arrow points to a button labeled 'Patient Required Fields'. To the right of this button are 'Save' and 'Cancel' buttons. Below the button, there are several empty text input fields. At the bottom right, there are 'Save' and 'Cancel' buttons.

Set the required fields for the patient prescription drug history and the patient prescription picklist queries.



The screenshot shows a dialog box titled 'Patient Required Fields'. It has two tabs: 'PPDH' (selected) and 'PPPL'. Under the 'PPDH' tab, there is a section titled 'Required Fields For Patient Drug History'. This section contains a list of checkboxes for various fields: Patient First Name, Patient Middle Name, Patient Last Name, Patient Name Suffix, Patient Sex Code, Patient Birth Date, Patient SSN ID, Patient Primary Contact Number, Patient Primary Contact Mailing Address, Patient Species Code, Patient Location Code, Patient Name Of Animal Text, Request Prescription Date Range, Patient Identifier, Patient Driver License, Patient Military, Patient National Health, Patient Other, Patient Passport, Patient Social Security Number, Patient State Issued, Patient Tribal, Patient Unique System, and Patient Vendor System. At the bottom, there is a 'Home State Priority' checkbox set to 'Disabled'. 'Save' and 'Cancel' buttons are at the bottom right.



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.

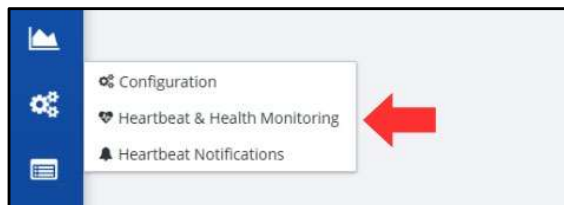
Home State Priority: ☐ Disabled

## 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.



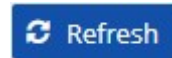
2. By default, you will be at the current site *SRS: Heartbeat and Health Monitoring* screen.



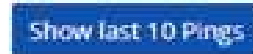
3. This screen includes various graphs to show the current status of the SRS.

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

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



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

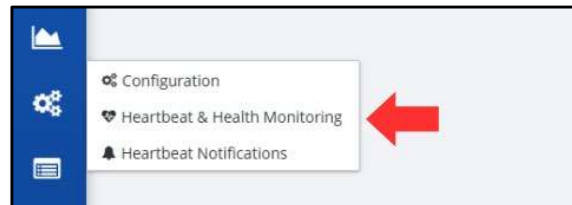
Graph Title	X-Axis	Y-Axis	Description
<b>Status Over a Period of Time With Timeline Bar</b>	Time	Status—Up/Down	The status of the SRS over a period of time.
<b>Instance Status</b>	Time	Status—Up/Down	The status of the SRS over a period of time, allows you to use the drop-down to switch the instance.
<b>JVM Threads</b>	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
<b>Garbage Collectors</b>	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.
<b>CPU</b>	Time	Percent usage	The amount of processing power used over time.
<b>JVM Memory</b>	Time	Size of JVM memory	Helps to detect trends such as memory growth, potential memory leaks, or inefficient memory usage patterns.
<b>Disk Space Used</b>	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.

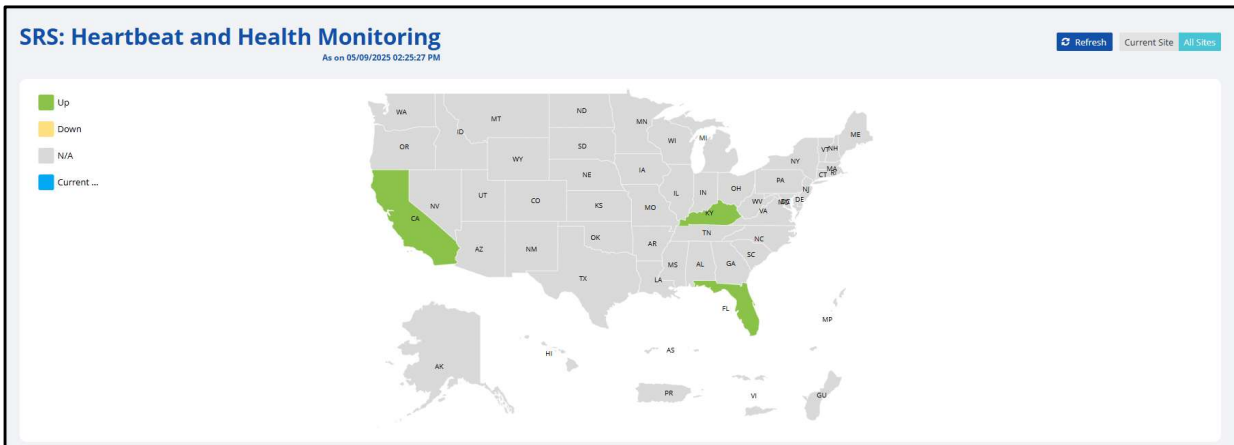
1. Click on the *State Routing Service* button, followed by the *Heartbeat & Health Monitoring* option, located on the left-hand side of the screen.



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



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



- 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.

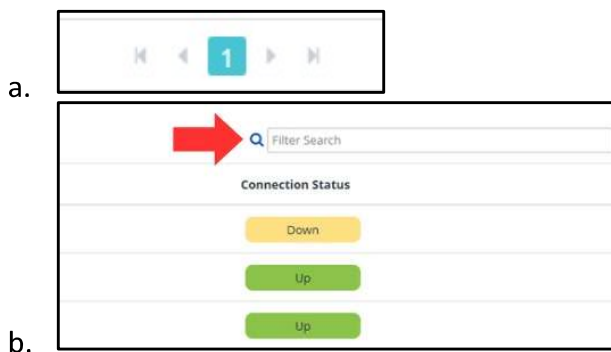


- Scrolling down on this screen, you are able to see a list of the states and their connection status in a table. The table also allows you to see the most recent query to or from a state.

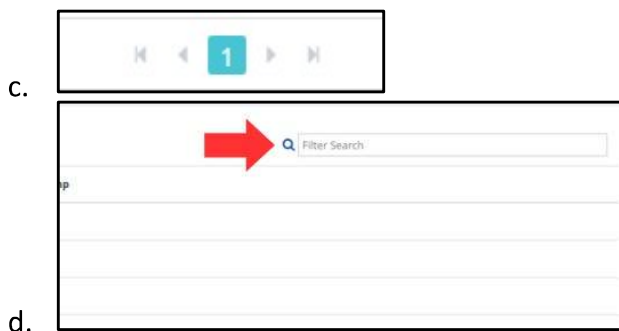
**Note:** The following table includes a description of each of the table headers.





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)	04/09/2023 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:
- Finding the state on the list using the page buttons under the table.
  - Searching for the state in the search box above the table.



7. Scrolling down further, the last table displays a list of the connected HCEs and the last time a query was received from them. An HCE can be found by:
- Using the page buttons on the bottom of the table and looking for the entity.
  - Searching for the site in the search bar above the table.



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

**PDMP Transaction Status Table**

Heading	Description
<b>Name</b>	Name and two-letter abbreviation for the state.
<b>From [State Code] (Outbound)</b>	The date and time of the last query from your state to listed state.
<b>To [State Code] (Inbound)</b>	The date and time of the last query from this state to the user's state.
<b>Connection Status</b>	The current status of that state's SRS.

## HCE Transaction Status to TT (Inbound)

Heading	Description
<b>Name</b>	The HCE code to identify the appropriate HCE.
<b>Last Transaction Timestamp</b>	The date and time of the last query from the HCE 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.

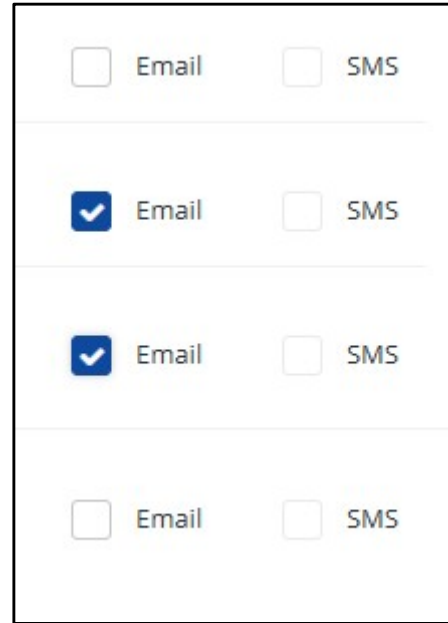
To navigate to the heartbeat notifications, follow the instructions below.

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

A screenshot of the 'SRS: Heartbeat Notification Subscriptions' configuration page. The page has a header with the RxCheck logo and 'Site Code(s): TT'. A left sidebar contains navigation icons. The main content area is titled 'SRS: Heartbeat Notification Subscriptions' and includes a 'Save' button. It contains four sections for configuring notifications: 'PDMP Connection', 'Your PDMP SRS', 'Performance', and 'Partnering PDMP SRS'. Each section has a description and checkboxes for 'Email' and 'SMS' notifications. At the bottom, there is an 'HCE Connection' section and an 'Integration SRS' section, also with 'Email' and 'SMS' checkboxes. The footer shows 'BJA RxConsole' and 'RxConsole 3.1.2 2803fcc7'.

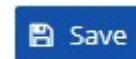
2. Select the desired boxes to subscribe to that notification.
  - a. If the *Email* option is checked, the user will receive emails to the mailbox associated with their RxConsole application login.
  - b. If the *SMS* option is checked, the user will receive text messages on the mobile phone number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



<input type="checkbox"/>	Email	<input type="checkbox"/>	SMS
<input checked="" type="checkbox"/>	Email	<input type="checkbox"/>	SMS
<input checked="" type="checkbox"/>	Email	<input type="checkbox"/>	SMS
<input type="checkbox"/>	Email	<input type="checkbox"/>	SMS

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

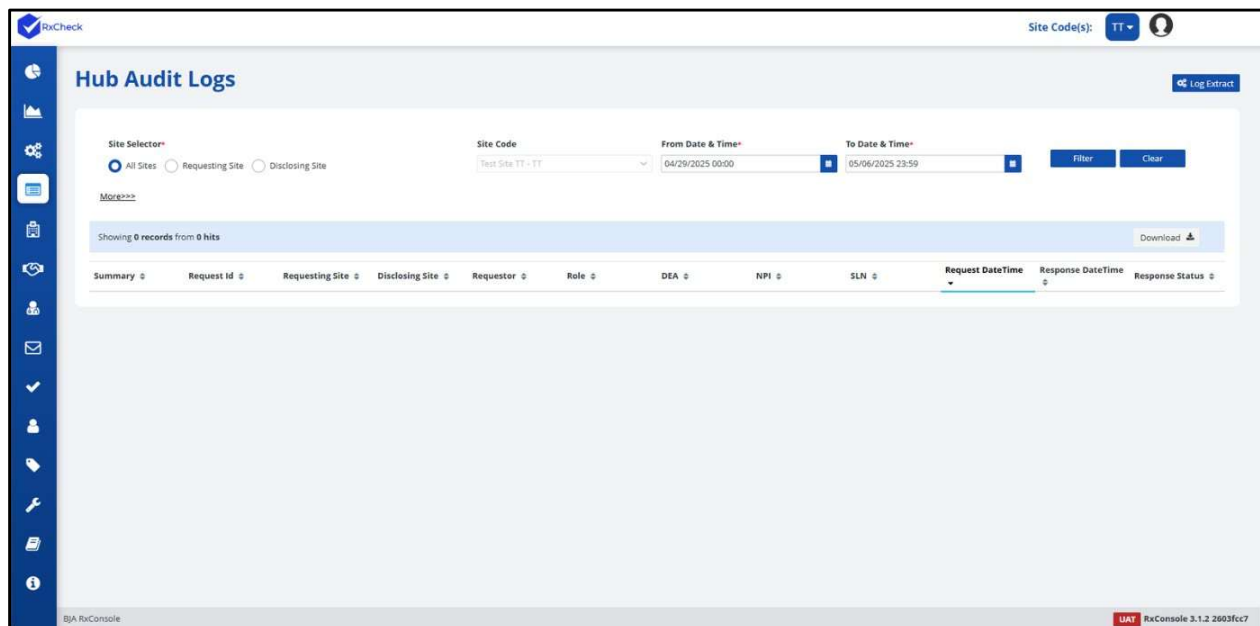
The Hub Audit Log captures detailed records of all incoming and outgoing transactions processed through the RxCheck Hub. This feature provides state PDMP administrators with visibility into:

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

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 5 records from 5 hits										Export Logs (SFTP)	Download
Summary	Request Id	Requesting Site	Disclosing Site	Requestor	Role	DEA	NPI	SLN	Request DateTime	Response DateTime	Response Status
<a href="#">View</a>	PMIX2-Tetrus LB3-RPT	QQ	TT		Prescriber Delegates - Licensed				11/20/2025 09:38:24AM	11/20/2025 09:38:24AM	NotFound
<a href="#">View</a>	PMIX2-Tetrus LB3-RPT	QQ	TT		Prescriber Delegates - Licensed				11/20/2025 09:28:46AM	11/20/2025 09:28:47AM	Disallowed

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

For example, clicking on *View* 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:42671e1d-49a5-45d3-8047-b124a81ec8a5		
Audit Id	3d9f6937-27f5-4105-9129-50c03c32a944		
Request Id	Pharmacy simulator test	Request Status	Connection Error
Requesting Site	QQ_ABC	Disclosing Site	TT
Requestor	test tetrus	Requestor Role	Pharmacy
Validation Type	--		
DEA#	12486040	NPI#	1700889730
SL#	21486040	OTHER#	--
PMIX Server Version	PMIX2		
Source Request	NCPDP2017071	Query Type	PPDH
Request Time	11/14/2025 04:49:28 AM	Response Time	11/14/2025 04:49:29 AM
SRS SiteCode	QQ_ABC	Vendor Name	--

**Error Log**

Http Status	500
Reason	EXCEPTION
Detail	Error : Server returned HTTP response code: 500 for URL: https://10.1.0.15:28443/rxinbound/service/pmix2
Message	<pre>&lt;soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"&gt;&lt;soap:Header&gt;&lt;Action xmlns="http://www.w3.org/2005/08/addressing"&gt;http://www.pmixpmp.org/pmp/ProvidePrescript ionDrugHistoryResponse&lt;/Action&gt;&lt;MessageID xmlns="http://www.w3.org/2005/08/addressing"&gt;urn:uuid:bb40bcf5-3e88-4b53-8f0c- e1334489c6aa&lt;/MessageID&gt;&lt;To xmlns="http://www.w3.org/2005/08/addressing"&gt;http://www.w3.org/2005/08/addressing/anonym ous&lt;/To&gt;&lt;RelatesTo xmlns="http://www.w3.org/2005/08/addressing"&gt;uuid:42671e1d-49a5-45d3- 8047-b124a81ec8a5&lt;/RelatesTo&gt;&lt;/soap:Header&gt;&lt;soap:Body&gt;&lt;soap:Fault&gt;&lt;soap:Code&gt; &lt;soap:Value&gt;soap:Receiver&lt;/soap:Value&gt;&lt;/soap:Code&gt;&lt;soap:Reason&gt;&lt;soap:Text xml:lang="en"&gt;Unable to find the Public Certificate for QQ_ABC&lt;/soap:Text&gt;&lt;/soap:Reason&gt; &lt;/soap:Fault&gt;&lt;/soap:Body&gt;&lt;/soap:Envelope&gt;</pre>

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

Title	Description
<b>Summary</b>	Provides details about the transaction and any errors.
<b>Request ID</b>	The ID provided in a request transaction that is made to obtain prescription data of an individual patient.
<b>Requesting Site</b>	The state code of the state that initiated the data request.
<b>Disclosing Site</b>	The state code of the state to which the data request is being sent to.
<b>Requestor</b>	The name of the healthcare professional who submitted the request.
<b>Role</b>	The role of the healthcare professional who submitted the request.
<b>DEA</b>	The DEA number of the healthcare professional who submitted the request.
<b>NPI</b>	The NPI number of the healthcare professional who submitted the request.
<b>SLN</b>	The state license number (SLN) of the healthcare professional who submitted the request.
<b>Request DateTime</b>	The date and time that the request was initiated.
<b>Response DateTime</b>	The date and time that the response was sent.
<b>Response Status</b>	The status of the transaction.

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

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

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

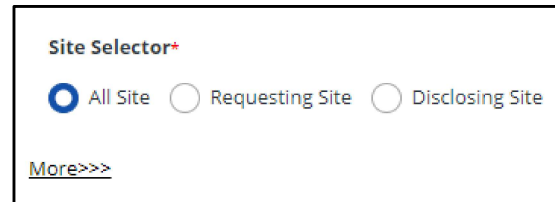
## 8.2. Filter the Hub Audit Logs

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.

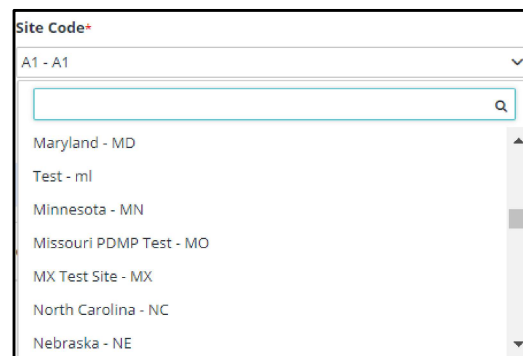


The image shows a form titled "Site Selector\*". It contains three radio button options: "All Site" (which is selected), "Requesting Site", and "Disclosing Site". Below the radio buttons is a link that says "More>>>".

**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 drop-down options and checking the box.
  - b. Typing in the search bar to filter results.

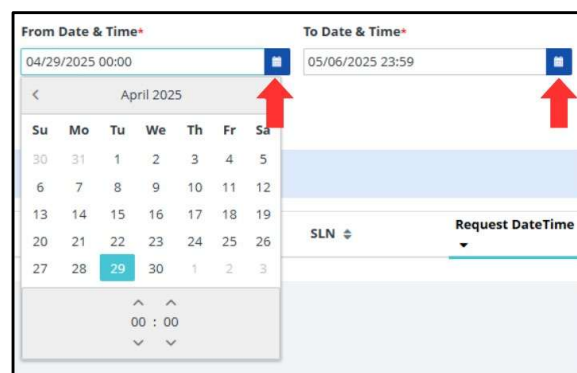
**Note:** This filter is only active when *Disclosing Site* or *Requesting Site* is selected in the *Site Selector* in step 2 above. This field is required.



The image shows a dropdown menu titled "Site Code\*". The current selection is "A1 - A1". Below the dropdown is a search bar with a magnifying glass icon. Below the search bar is a list of states: Maryland - MD, Test - ml, Minnesota - MN, Missouri PDMP Test - MO, MX Test Site - MX, North Carolina - NC, and Nebraska - NE.

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).



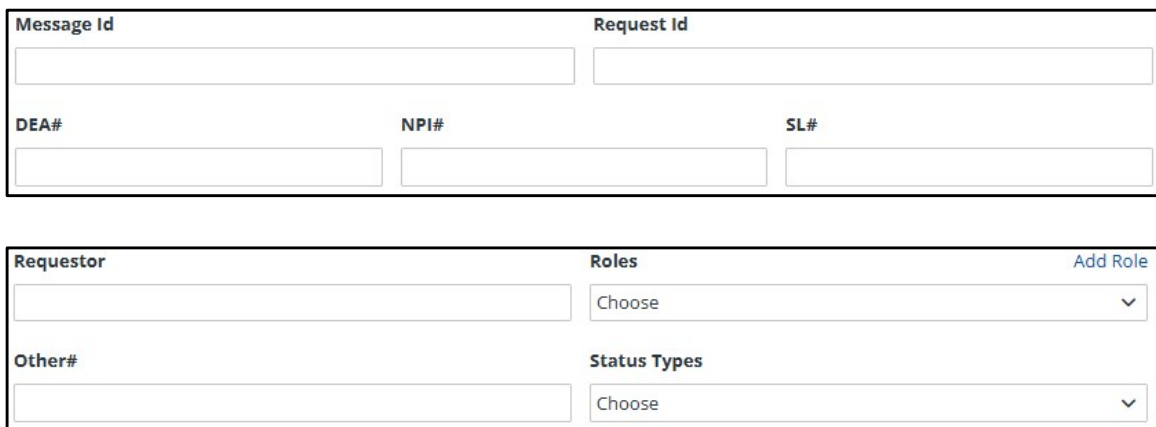
The image shows a date and time range selection interface. It has two main sections: "From Date & Time\*" and "To Date & Time\*". The "From Date & Time\*" section shows a date of "04/29/2025 00:00" and a blue calendar icon. The "To Date & Time\*" section shows a date of "05/06/2025 23:59" and a blue calendar icon. Below the "From Date & Time\*" section is a calendar for April 2025. The calendar shows days of the week (Su, Mo, Tu, We, Th, Fr, Sa) and dates (30, 31, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 1, 2, 3). The date "29" is highlighted. Below the calendar are up/down arrows for the time (00:00). Below the "To Date & Time\*" section is a "Request DateTime" dropdown menu.

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

The image shows a 'Site Selector' filter interface. It has three radio buttons: 'All Sites' (selected), 'Requesting Site', and 'Disclosing Site'. Below the radio buttons is a link labeled 'More>>>' with a red arrow pointing to it from the right.

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. Other#
  - i. 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.

The image shows a form with two sections. The top section has four input fields: 'Message Id', 'Request Id', 'DEA#', and 'NPI#'. The bottom section has four input fields: 'Requestor', 'Roles' (with a dropdown menu), 'Other#', and 'Status Types' (with a dropdown menu). There is an 'Add Role' link next to the 'Roles' dropdown.

7. Click on the *Filter* button to apply the selected Hub Audit Log criteria.

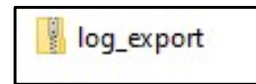
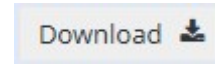
A blue rectangular button with the word 'Filter' in white text.

## 8.3. Download the Hub Audit Logs

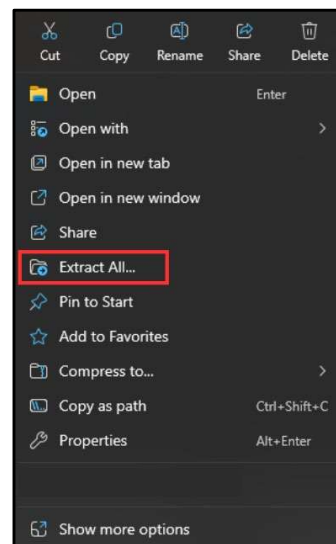
The RxConsole application allows PDMP administrators to download a copy of their audit logs. When downloaded, the audit logs are packaged as a zipped file.

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.



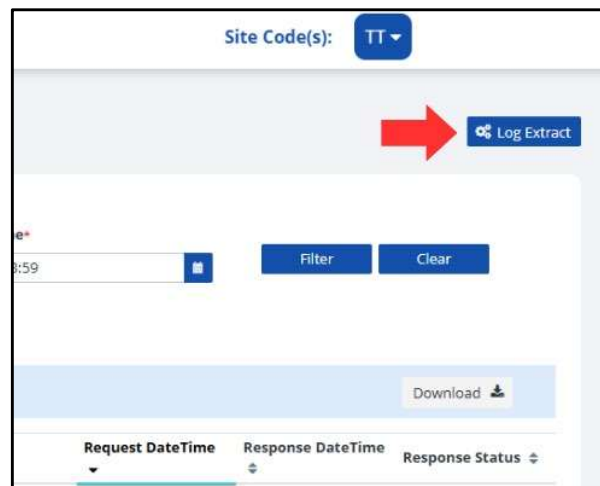
4. Right-click on the zipped folder to view options



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
<b>Host Name</b>	The domain name or IP address of the remote sFTP server. Example: sftp.example.com or 192.168.1.100.
<b>Port</b>	The port number used for the sFTP connection. The default is “22,” but it can be configured to other values by the server administrator.
<b>File Path</b>	The directory path on the remote server where files will be uploaded to or downloaded from. Example: /home/sftp, /user/uploads, or /data/incoming.
<b>Username</b>	The login name used to authenticate the user with the sFTP server. It is typically assigned by the server administrator.
<b>Password</b>	The secret key or password corresponding to the username for authentication. This can be omitted if key-based authentication is used.
<b>Active</b>	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.

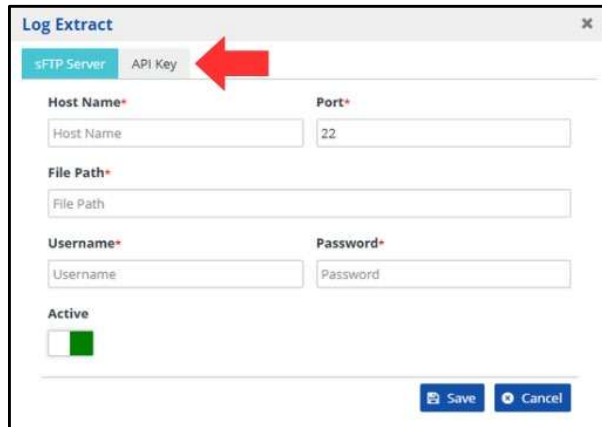
After the sFTP configuration is saved, the system will activate the *Export Logs (sFTP)* button for the PDMP administrator. To initiate the log export, click this button. The system will process the request and send an email notification once the export is complete.



## 8.5. Using an API to Download the Logs

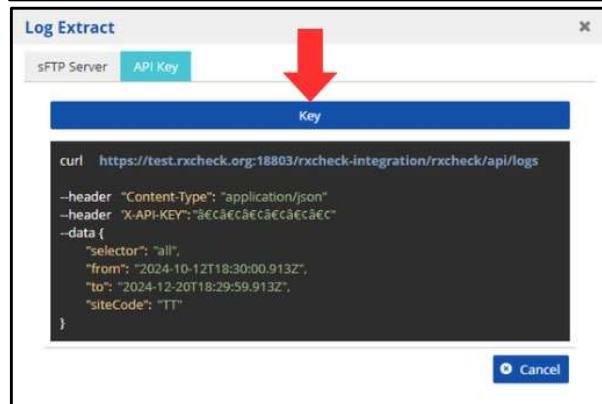
RxConsole also allows a PDMP administrator to enable an API endpoint to download audit logs from the RxCheck Hub. To access this API, an API key is required.

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



The screenshot shows the 'Log Extract' window with the 'API Key' tab selected, indicated by a red arrow. The window contains fields for 'Host Name\*', 'Port\*', 'File Path\*', 'Username\*', and 'Password\*'. There is also an 'Active' checkbox and 'Save' and 'Cancel' buttons at the bottom right.

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



The screenshot shows the 'Log Extract' window with the 'API Key' tab selected. A red arrow points to the 'Key' button. Below the button, a sample API request is displayed in a dark box. The request is a curl command for the URL 'https://test.rxcheck.org:18803/rxcheck-integration/rxcheck/api/logs' with headers for 'Content-Type' and 'X-API-KEY', and a data object containing 'selector', 'from', 'to', and 'siteCode'.

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. HCEs

An HCE refers to any licensed healthcare provider or organization that is authorized by its respective state to deliver professional healthcare services. This includes:

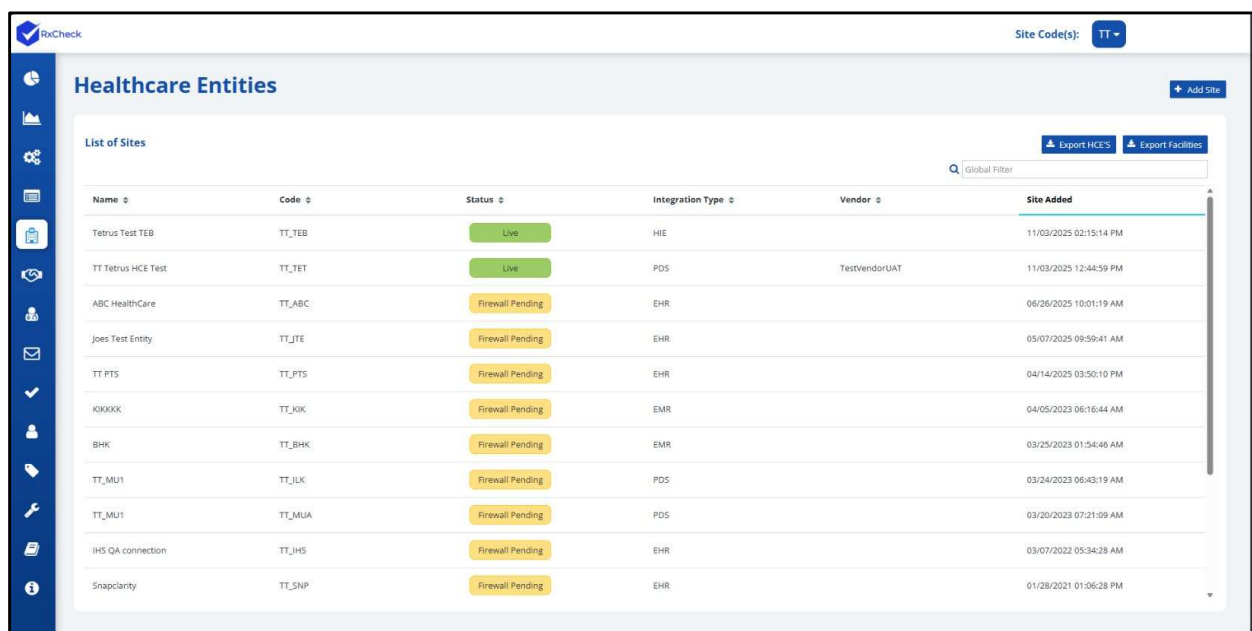
- Individual providers licensed to practice healthcare.
- Healthcare organizations employing licensed professionals.
- eHealth exchange organizations recognized by the state for providing licensed healthcare services.

An HCE 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 HCE 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 HCEs page.

Administrators can also view and manage existing HCE 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 HCEs within a state's PDMP system. The accompanying table provides definitions for each column heading shown in the interface.



The screenshot shows the RxCheck interface for Healthcare Entities. The page title is "Healthcare Entities" and there is a "Site Code(s): TT" dropdown in the top right. A "+ Add Site" button is also present. Below the title is a "List of Sites" section with a search bar and "Export HCE's" and "Export Facilities" buttons. The table below lists various sites with their status and integration types.

Name	Code	Status	Integration Type	Vendor	Site Added
Tetrus Test TEB	TT_TEB	Live	HIE		11/03/2025 02:15:14 PM
TT Tetrus HCE Test	TT_TET	Live	PDS	TestVendorUAT	11/03/2025 12:44:59 PM
ABC HealthCare	TT_ABC	Firewall Pending	EHR		06/26/2025 10:01:19 AM
Joes Test Entity	TT_JTE	Firewall Pending	EHR		05/07/2025 09:59:41 AM
TT PTS	TT_PTS	Firewall Pending	EHR		04/14/2025 03:50:10 PM
KROXXX	TT_KOK	Firewall Pending	EMR		04/05/2023 06:16:44 AM
BHK	TT_BHK	Firewall Pending	EMR		03/25/2023 01:54:46 AM
TT_MU1	TT_JLK	Firewall Pending	PDS		03/24/2023 06:43:19 AM
TT_MU1	TT_MUA	Firewall Pending	PDS		03/20/2023 07:21:09 AM
IHS QA connection	TT_IHS	Firewall Pending	EHR		03/07/2022 05:34:28 AM
Snapclarity	TT_SNP	Firewall Pending	EHR		01/28/2021 01:06:28 PM

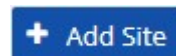
Heading	Description
<b>Name</b>	The name of the HCE.
<b>Code</b>	A six-character code that follows the following format: <ul style="list-style-type: none"> <li>• Two letters to represent the state code.</li> <li>• An underscore (_).</li> <li>• Three letters to represent an HCE site.</li> </ul>
<b>Status</b>	Indicates the current status of an HCE. <ul style="list-style-type: none"> <li>• Active: The HCE is currently active.</li> <li>• Inactive: The HCE is currently inactive.</li> <li>• Firewall Pending: The HCE is currently active but was recently set up.</li> </ul>
<b>Integration Type</b>	Refers to the site type value that was selected when the HCE was created. This value will be displayed as one of the following: <ul style="list-style-type: none"> <li>• EHR</li> <li>• Electronic Medical Records (EMR)</li> <li>• HIE</li> <li>• Pharmacy Dispensing System (PDS)</li> </ul>
<b>Vendor</b>	The integration vendor for the HCE.
<b>Site Added</b>	Date and time when the HCE site was created.

## 9.1. Add a New HCE Site

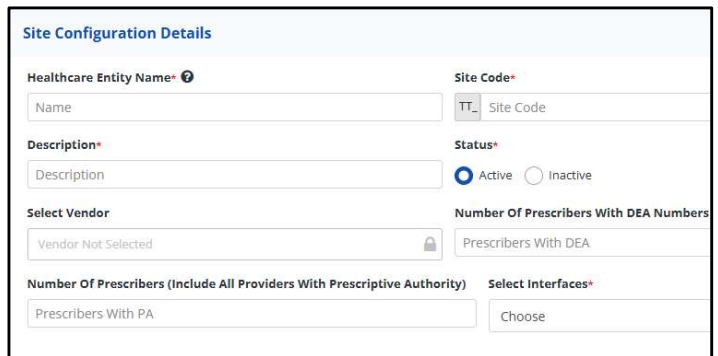
1. Click on the *Healthcare Entities* button, located on the left-hand side of the screen.




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



3. Populate the site configuration details for the new HCE. Refer to the [“Breakdown of Healthcare Entity Site Details”](#) section below for field-specific guidance.




**Site Configuration Details**

Healthcare Entity Name\* 

Site Code\*

Description\*

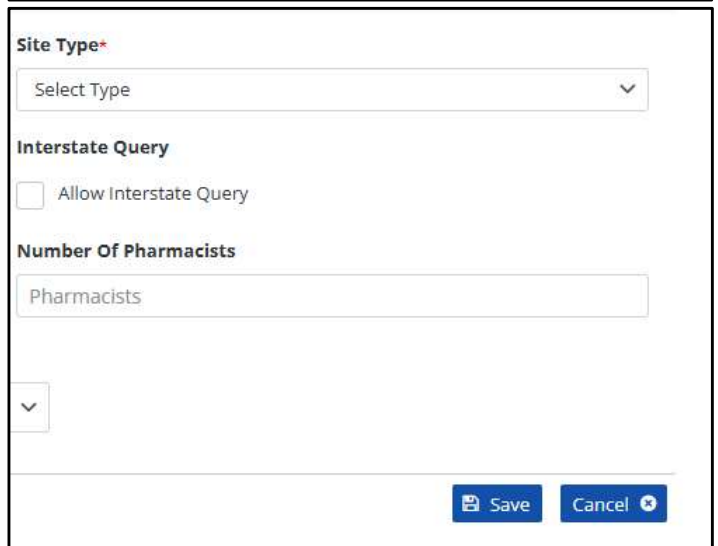
Status\* ☒ Active ☐ Inactive


Select Vendor  

Number Of Prescribers With DEA Numbers

Number Of Prescribers (Include All Providers With Prescriptive Authority)

Select Interfaces\*




**Site Type\***  

**Interstate Query**

☐ Allow Interstate Query

**Number Of Pharmacists**



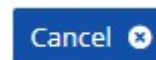
4. To populate the “Select Vendor” field, you must first click on the small lock symbol within the field.



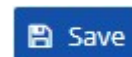
**Select Vendor**



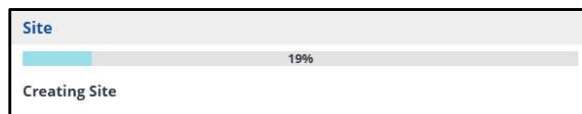
5. To exit without saving, click the *Cancel* button.



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



7. Wait patiently as your site is being created.

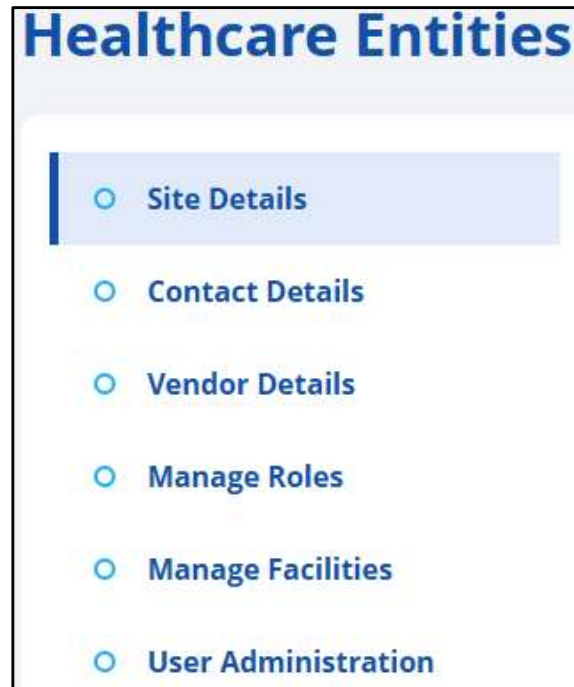


**Site**

Creating Site

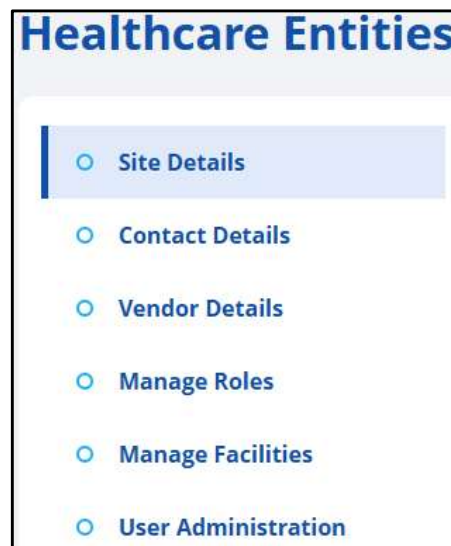
8. Populate additional details as requested in the corresponding data fields for each section.

Refer to the “[Breakdown of Healthcare Entity Site Details](#)” section below for field-specific guidance.



## 9.2. Breakdown of HCE Site Details

Once an HCE 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 an HCEs record.

## 9.2.1. Site Details

This section displays information related to this specific HCE.

Site Configuration Details

Healthcare Entity Name\*

Joes Test Entity

Site Code\*

TT\_JTE

Site Type\*

EHR

Description\*

Small rural hospital

Status\*

☒ Active
 ☐ Inactive

Interstate Query

☐ Allow Interstate Query

Select Vendor

Vendor Not Selected

Number Of Prescribers With DEA Numbers

1

Number Of Pharmacists

1

Number Of Prescribers (Include All Providers With Prescriptive Authority)

1

Select Interfaces\*

1 items selected

Heading	Description
<b>Healthcare Entity Name</b>	The name of the HCE.
<b>Site Code</b>	<p>A six-character code that follows the following format:</p> <ul style="list-style-type: none"> <li>Two letters to represent the state code. This is auto-populated.</li> <li>An underscore (_).</li> <li>Three letters to represent an HCE site. These are entered by the PDMP administrator.               <ul style="list-style-type: none"> <li>When deciding on the three letters to represent an 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.</li> <li>Example: Walmart may be <b>WLT</b> or <b>WAL</b>, where Walgreens may be <b>WGN</b> or <b>WAL</b>.</li> </ul> </li> </ul>
<b>Site Type</b>	<p>Refers to the site type. This value can be set as one of the following:</p> <ul style="list-style-type: none"> <li>EHR</li> <li>EMR</li> <li>HIE</li> <li>PDS</li> </ul>
<b>Description</b>	A simple description of the HCE site.
<b>Status</b>	Status that indicates if a site is active or inactive.
<b>Interstate Query</b>	When checked, the HCE will be able to send interstate data requests.
<b>Select Vendor</b>	The integration vendor providing services to this HCE.

Heading	Description
<b>Number of Prescribers With DEA numbers</b>	A count of prescribers with DEA numbers at that HCE.
<b>Number of Pharmacists</b>	A count of pharmacists at that HCE.
<b>Number of Prescribers (Include All Providers With Prescriptive Authority)</b>	A count of all prescribers at that HCE.
<b>Select Interfaces</b>	<p>The type of connection the HCE is using to connect to RxCheck or a third-party integrator. The following options are available:</p> <ul style="list-style-type: none"> <li>• NCPDP2017</li> <li>• HTML</li> <li>• FHIR3</li> <li>• FHIR4</li> <li>• PMIX2</li> <li>• JSON</li> </ul>

### 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.

Site Contact Details

PRIMARY CONTACT DETAILS:

First Name

Last Name

Phone Number

Extension

Email

SECONDARY CONTACT DETAILS:

First Name

Last Name

Phone Number

Extension

Email

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

### 9.2.3. Vendor Details

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

**SRS Hosting Details**

Integration managed by\*

☒ HCE IT ☐ STATE ☐ VENDOR

**SRS Hosting Details**

Integration managed by\*

☐ HCE IT ☐ STATE ☒ VENDOR

Where is it Hosted

☐ HCE IT INFRA ☐ Vendor IT INFRA ☐ Private Cloud ☐ Government Cloud

Vendor Name

Vendor Address

Vendor Contact

Are the servers being accessed outside of the US?

☐ Yes ☒ No

Heading	Description
<b>HCE IT</b>	This option indicates that the IT team of the HCE oversees the SRS hosting and managing responsibilities.
<b>State</b>	This option indicates that the IT team of the state oversees the SRS hosting and managing responsibilities.
<b>Vendor</b>	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
<b>Where Is It Hosted</b>	Refers to where the vendor hosts the SRS server for the HCE. The following options can be selected. <ul style="list-style-type: none"><li>• HCE IT INFRA—Hosted by the HCE's infrastructure.</li><li>• Vendor IT INFRA—Hosted by the vendor's infrastructure.</li><li>• Private cloud—Hosted on a private cloud, accessible by only the HCE and/or vendor.</li><li>• Government cloud—Hosted on a government cloud, accessed by individuals outside the HCE or state PDMP team.</li></ul>
<b>Vendor Name</b>	The name of the vendor hosting the SRS.

Heading	Description
<b>Vendor Address</b>	The address of the vendor hosting the SRS.
<b>Vendor Contact</b>	The name of the contact responsible for managing the SRS.
<b>Are the Servers Being Accessed Outside the United States?</b>	A <i>Yes</i> or <i>No</i> 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 an HCE to submit prescription data requests. Roles are assigned by selecting the appropriate tags associated with the HCE.

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
<b>Assign All</b>		Automatically selects all displayed roles.
<b>Clear All</b>		Automatically deselects all displayed roles.
<b>Show List</b>		Will display all available roles in two separate lists, an <i>Authorized Roles</i> list and a <i>Selected Roles</i> list.
<b>Hide List</b>		Will display all available roles as tags (default). <b>Note:</b> 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.



Authorized Roles			Selected Roles
Advanced Practice RNs	>	<	Dentists
Dispenser Delegates - Licensed	>	<	Pharmacists
Dispenser Delegates - Unlicensed	>	<	Optometrists
Homeopaths	>		
Interns	>		
Naturopaths	>		
Other Non-Prescribers	>		
Other Prescribers	>		
Pharmacy	>		
Physician Assistants	>		

### 9.2.5. Manage Facilities

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

<b>Facilities</b>	<a href="#">Add Facility</a>	<a href="#">Add Multiple Facilities</a>
No Facility Data Exists for this HCE.		

There are two buttons available to an RxConsole user.

Button Name	Button Image	Functionality
<b>Add Facility</b>		Will display the <i>Facility</i> pop-up to enter a single facility.
<b>Add Multiple Facilities</b>		Will redirect the PDMP administrator to the <i>Add Facilities</i> page.

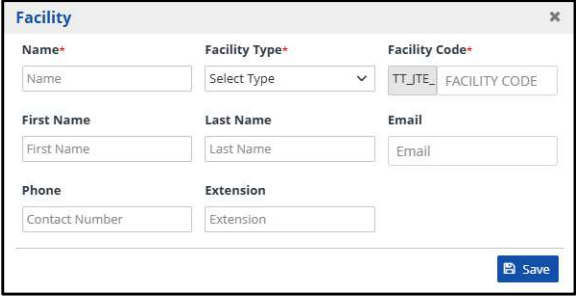
#### 9.2.5.1. How to Add a Single Healthcare Facility

1. Click on the *Add Facility* button.



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

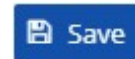
To see a description of each field, see the table below.



The 'Facility' pop-up window contains the following fields:

- Name\***: Text input field.
- Facility Type\***: Dropdown menu with 'Select Type'.
- Facility Code\***: Text input field with 'TT\_JTE' and 'FACILITY CODE'.
- First Name**: Text input field.
- Last Name**: Text input field.
- Email**: Text input field.
- Phone**: Text input field with 'Contact Number'.
- Extension**: Text input field.
- Save**: Blue button with a save icon.

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



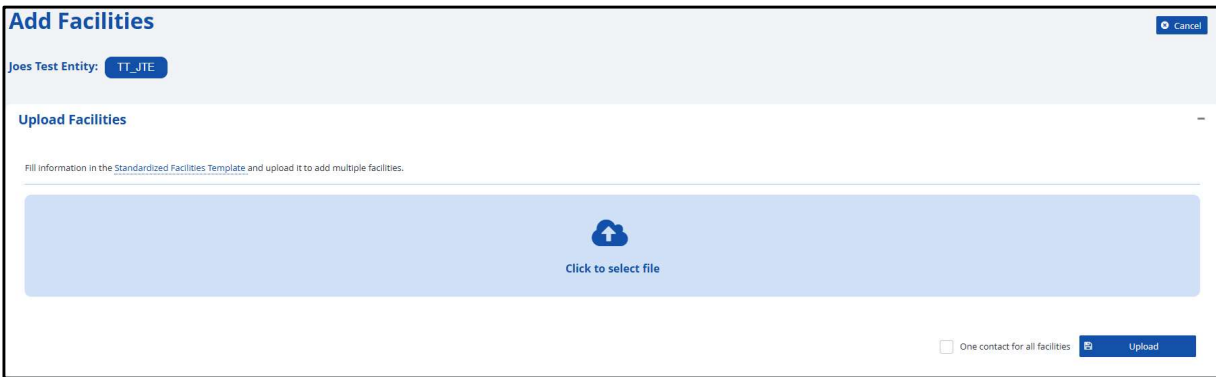
Heading	Description
<b>Name</b>	Individual facility's name.
<b>Facility Type</b>	Individual facility type. Options include: <ul style="list-style-type: none"> <li>• EHR</li> <li>• PDS</li> </ul>
<b>Facility Code</b>	Code specific to this individual facility. The HCE code is auto-populated, but the facility code is entered as an alphanumeric value.
<b>First Name</b>	Contact person's first name at this individual facility.
<b>Last Name</b>	Contact person's last name at this individual facility.
<b>Email</b>	Contact person's email at this individual facility.
<b>Phone</b>	Contact person's phone number at this individual facility.
<b>Extension</b>	Contact person's phone number extension at this individual facility, if any.

#### 9.2.5.2. How to Add Multiple Healthcare Facilities

- Click on the *Add Multiple Facilities* button.



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

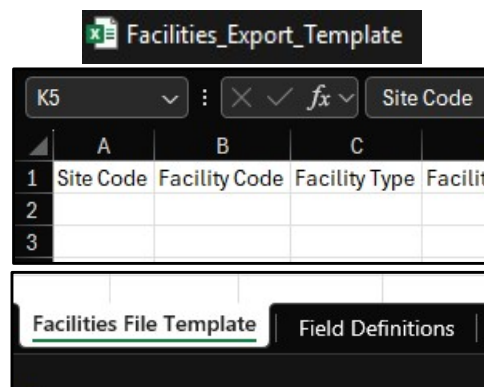


The 'Add Facilities' screen displays the following elements:

- Header**: 'Add Facilities' title and a 'Cancel' button.
- Entity**: 'Joes Test Entity: TT\_JTE'.
- Section**: 'Upload Facilities'.
- Instructions**: 'Fill information in the Standardized Facilities Template and upload it to add multiple facilities.'
- Upload Area**: A large blue box with a cloud upload icon and the text 'Click to select file'.
- Footer**: A checkbox labeled 'One contact for all facilities' and an 'Upload' button.

- 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 screenshot shows an Excel workbook titled "Facilities\_Export\_Template". The active tab is "Facilities File Template". The worksheet has columns labeled A, B, and C. Row 1 contains headers: "Site Code" in column A, "Facility Code" in column B, and "Facility Type" in column C. Rows 2 and 3 are empty. The bottom of the screenshot shows the "Field Definitions" tab.

	A	B	C
1	Site Code	Facility Code	Facility Type
2			
3			

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



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

- Press the *Click to Select File* button to choose the populated template to upload into the system.



- 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.

☐ One contact for all facilities

**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.

First Name*	Last Name*	Email
<input type="text"/>	<input type="text"/>	<input type="text"/>
Phone	Extension	
<input type="text"/>	<input type="text"/>	

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



- 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.

HCE Users <span style="float: right;">+ Add User</span>				
Email	Name	Site Name	Status	User Type
m@email.com	m s	TT_RWJ	Active	SUB_ADMIN

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

A state PDMP administrator is allowed to add a new administrative user for an HCE following the steps below.

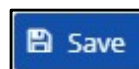
- Click the *Add User* button to open a pop-up window.



2. In the pop-up 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.



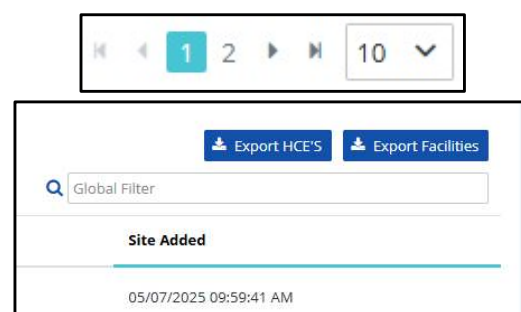
Heading	Description
<b>Email</b>	The contact email for the HCE user and username for RxConsole.
<b>Password</b>	The password for the HCE user to access the RxConsole application.
<b>Site Code</b>	The site code for the HCE user. This field will be auto-populated.
<b>First Name</b>	The HCE user's first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

### 9.3. Open an HCE Record

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



2. Find the HCE 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.



Healthcare Entities				
List of Sites				
Name	Code	Status	Integration Type	Site Added
Joes Test Entity	TT_JTE	Firewall Pending	EHR	05/07/2025 09:58:41 AM
TT PTS	TT_PTS	Firewall Pending	EHR	04/14/2025 03:50:10 PM
KXXXXK	TT_KIK	Firewall Pending	EMR	04/05/2023 06:16:44 AM
BHK	TT_BHK	Firewall Pending	EMR	03/25/2023 01:54:46 AM
TT_MU1	TT_JLK	Firewall Pending	POS	03/24/2023 06:43:19 AM
TT_MU1	TT_MUA	Firewall Pending	POS	03/20/2023 07:21:09 AM
IHS QA connection	TT_IHS	Firewall Pending	EHR	03/07/2022 05:34:28 AM
Snapclarity	TT_SNP	Firewall Pending	EHR	01/28/2021 01:06:28 PM
RWHI	TT_RHI	Firewall Pending	EHR	01/28/2021 10:29:35 AM
eHealth Exchange	TT_EHX	Firewall Pending	HIE	06/18/2020 02:49:57 PM

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

List of Sites

Name

Joes Test Entity

TT PTS

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

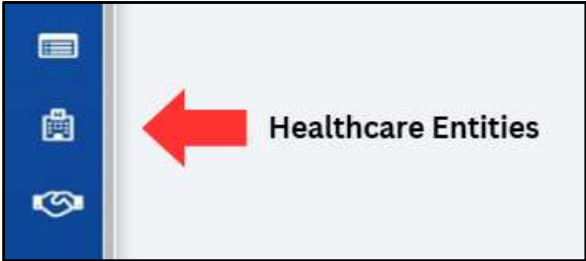
Save

Cancel

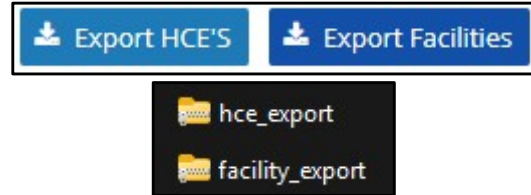
### 9.4. Export a List of Your HCEs and Facilities

RxConsole supports the ability for a state PDMP administrator to export a list of their HCEs and the facilities under those HCEs.

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

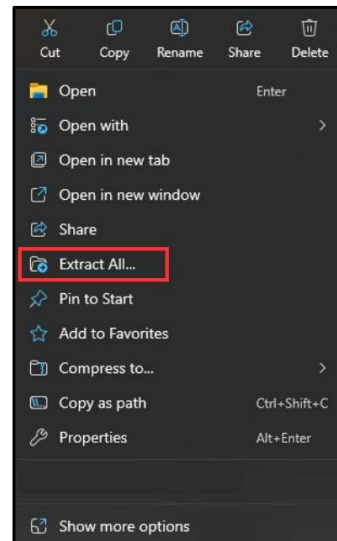


2. In the top-right corner, there are two buttons to extract either:
  - Export HCEs—Downloads a list of HCEs, their HCE code, and their status.
  - Export Facilities—Downloads a list of facilities, their site code, and their status.



**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
<b>Code</b>	A six-character code that follows the following format: <ul style="list-style-type: none"> <li>• Two letters to represent the state code.</li> <li>• An underscore (_).</li> <li>• Three letters to represent an HCE site.</li> </ul>
<b>Name</b>	The name of the HCE.
<b>Status</b>	Status that indicates if a site is active or inactive.

### Facility Export Columns

Heading	Description
<b>Code</b>	A facility code specific to that individual healthcare facility.
<b>Name</b>	The name of the facility.
<b>Status</b>	Status that indicates if the facility is active or inactive.



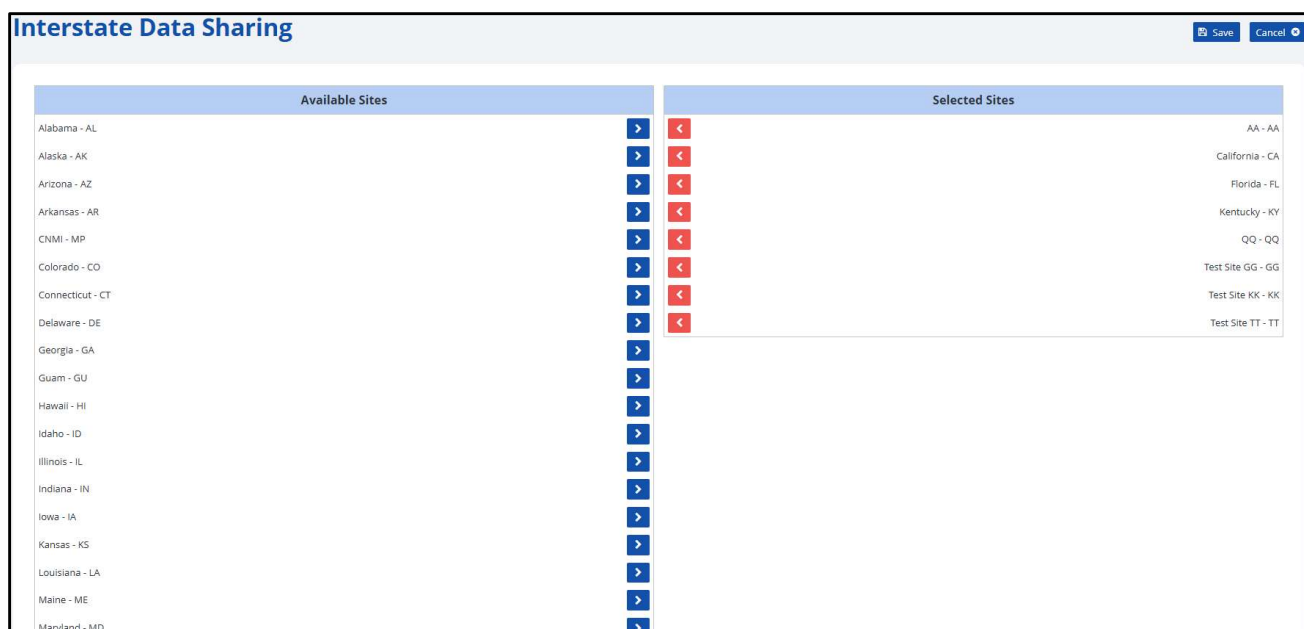
## 10. Interstate Data Sharing

The Interstate Data Sharing feature enables state PDMP administrators to designate which states 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 states 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.

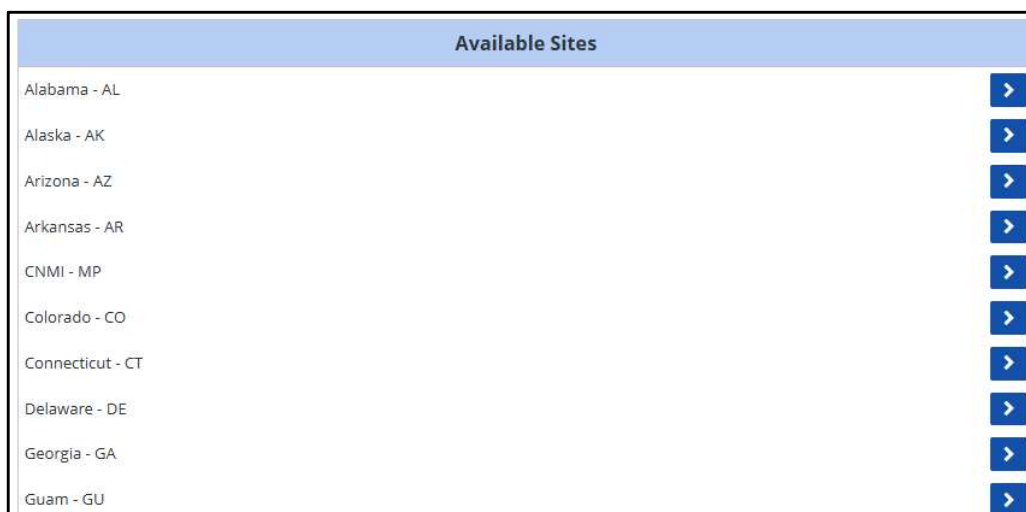
The following subsections provide step-by-step instructions for selecting and deselecting sites for interstate data sharing within the RxConsole Application. Each step is accompanied by a screenshot for visual reference.

## 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 that you would like to add for interstate data sharing.



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

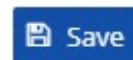


4. Verify that the site has moved from the *Available Sites* list on the left to the *Selected Sites* list on the right.

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



- 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

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



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

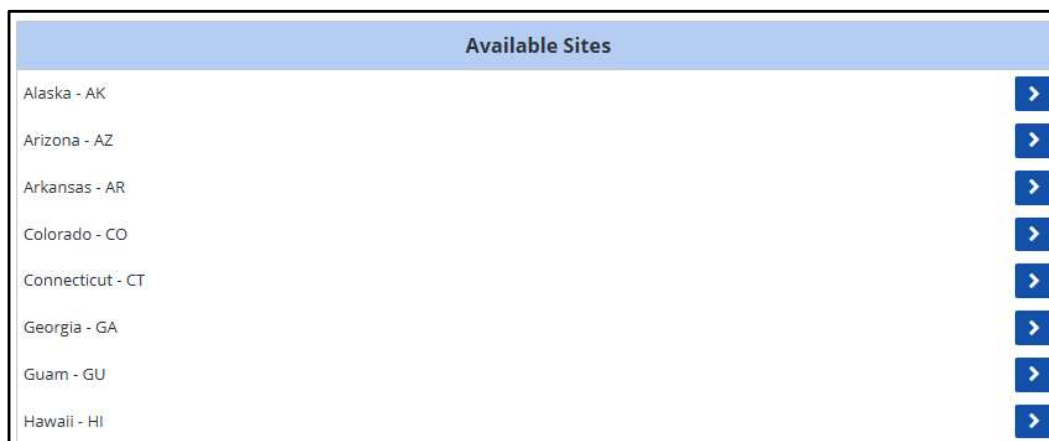


3. Click on the orange arrow button aligned with the desired site.

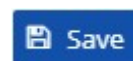


4. Verify that the site has moved from the *Selected Sites* list on the right to the *Available Sites* list on the left.

**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 an 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.

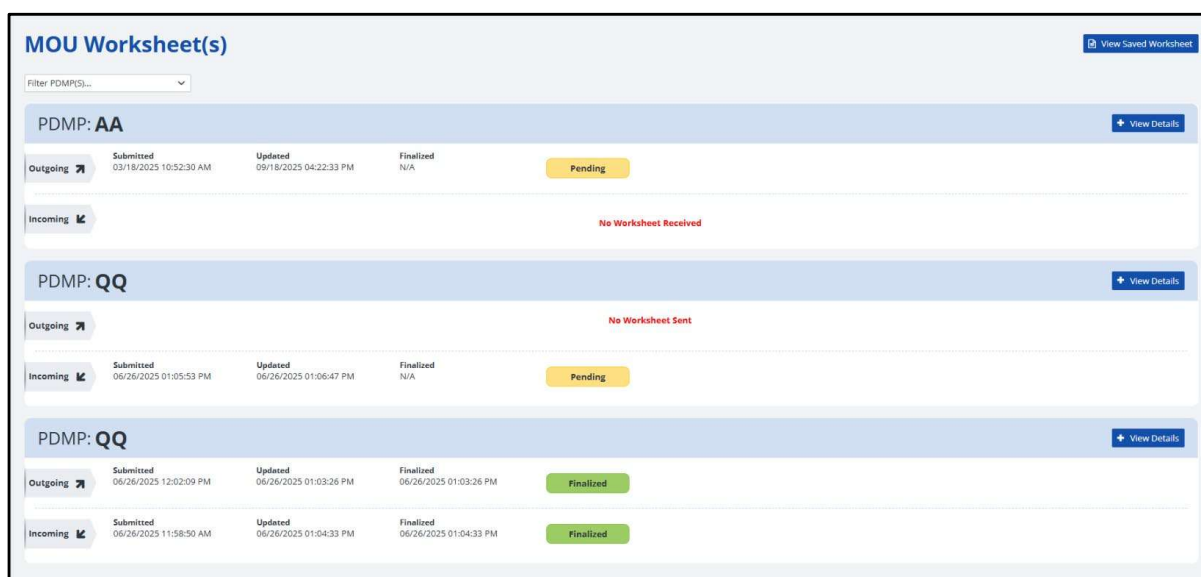
**Note:** This is an MOU worksheet, not a contract.

### 10.3.1 Populate and Submit the MOU Worksheet

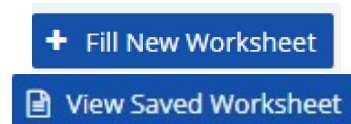
1. Click on the *Interstate Data Sharing* button, followed by the *MOU Worksheet(s)* option, located on the left-hand side of the screen.



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



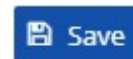
3. Click on the *Fill New Worksheet* button (if you have not completed a worksheet yet) or *View Saved Worksheet* (if you have previously completed a worksheet).



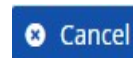
4. On the new *MOU Worksheet* page, populate the following sections:
  - State administration's information
  - User validation procedures
  - Data access and security
  - Data elements for request submissions
  - Query response
  - Miscellaneous

**Note:** Fields with a red asterisk (\*) are required.

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



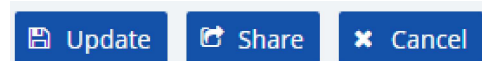
6. Alternatively, you can press the *Cancel* button to discard the changes and return to the previous screen.



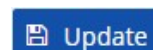
7. After saving, the *View Saved Worksheet* button will be displayed.



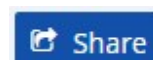
8. Click on *View Saved Worksheet* button to view the saved MOU worksheet. PDMP administrators can update the contents and/or share the MOU worksheet with other state(s).



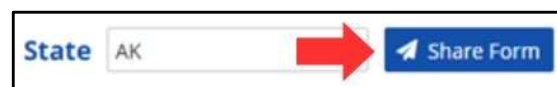
9. To edit the worksheet, click on the *Update* button.



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



11. Select a state from the drop-down 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.

**MOU Worksheet(s)** View Saved Worksheet

Filter PDMP(S):

**PDMP: AK** View Details

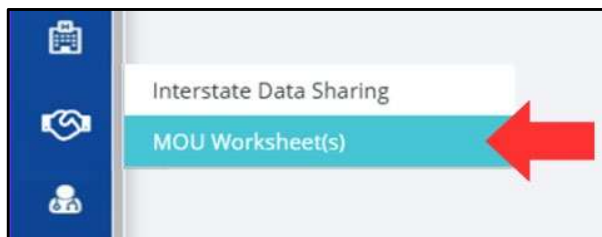
Submitted	Updated	Finalized
04/04/2025 03:39:30 PM manisha.pardeshi@tetruscor...	04/04/2025 03:39:30 PM manisha.pardeshi@tetruscor...	N/A

**Outgoing** ↗ Pending

**Incoming** ↖ No Worksheet Received

### 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 an interstate data sharing request.

**MOU Worksheet(s)** Fill New Worksheet

**PDMP: MD** View Details

**Outgoing** ↗ No Worksheet Sent

Submitted	Updated	Finalized
04/04/2025 03:39:30 PM manisha.pardeshi@tetruscor...	04/04/2025 03:39:30 PM manisha.pardeshi@tetruscor...	N/A

**Incoming** ↖ Pending

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](#).

+ **View Details**

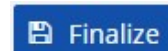
4. Click the *Cancel* button to discard the MOU worksheet data.



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.

MOU Worksheet(s)					+ Fill New Worksheet
PDMP: MD					+ View Details
Outgoing ↗					No Worksheet Sent
Incoming ↙	Submitted 04/04/2025 03:39:30 PM manisha.pardeshi@tetruscor...	Updated 04/04/2025 04:03:05 PM manisha.pardeshi@tetruscor...	Finalized 04/04/2025 04:03:05 PM manisha.pardeshi@tetruscor...	Finalized	

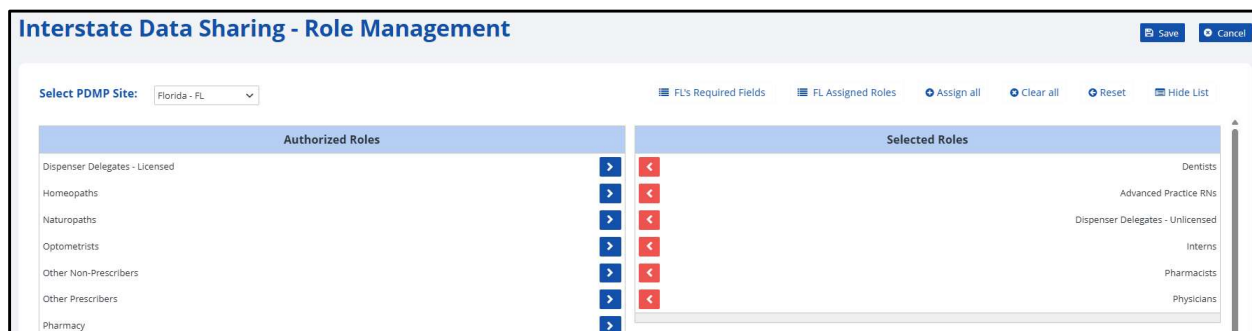


## 11. Interstate Data Sharing—Role Management

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.

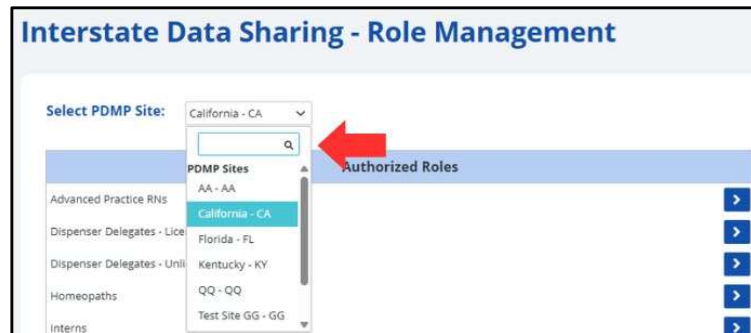
### 11.1. Select Roles for Interstate Data Sharing

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



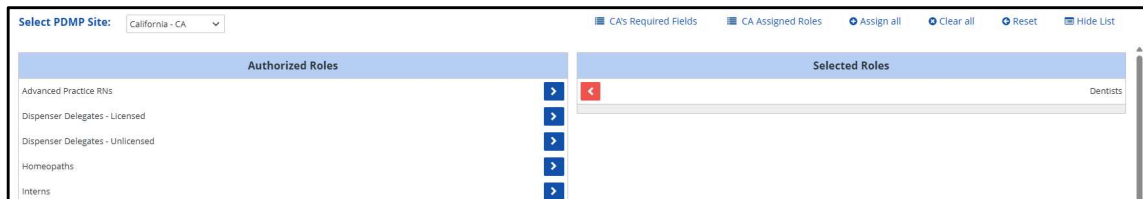
2. Select the PDMP site that you would like to manage a role for by selecting the downward-facing arrow in the box labeled *Select PDMP Site*. A user can find a site by:

- Scrolling through the list in the drop-down.
- Entering the name or state code for the desired state in the drop-down search box.



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

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



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

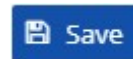


5. Verify that the role has moved from the *Authorized Roles* list on the left to the *Selected Roles* list on the right.

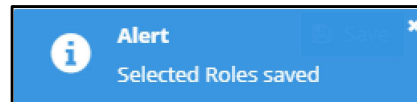


**Note:** Recently moved roles are not listed alphabetically and will instead appear at the bottom of the *Selected Roles* list.

- 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

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



- Select the PDMP site that you would like to manage a 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 drop-down.
  - Entering the name or state code for the desired state in the drop-down search box.

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



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

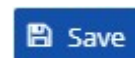
4. Click on the orange arrow button aligned with the desired role.



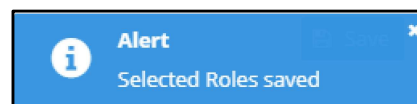
5. Verify that the role has moved from the *Selected Roles* list on the right to the *Authorized Roles* list on the left.

**Note:** Recently moved roles are not listed alphabetically and will instead appear at the bottom of the *Authorized 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.”



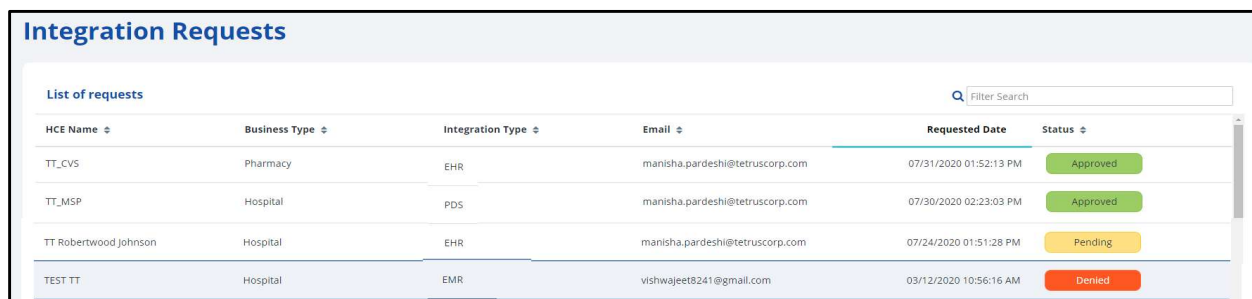
## 12. Integration Requests

The integration requests feature enables state PDMP administrators to view and manage connection requests submitted by HCEs within their state.

HCEs 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.



HCE Name	Business Type	Integration Type	Email	Requested Date	Status
TT_CVS	Pharmacy	EHR	manisha.pardeshi@tetruscorp.com	07/31/2020 01:52:13 PM	Approved
TT_MSP	Hospital	PDS	manisha.pardeshi@tetruscorp.com	07/30/2020 02:23:03 PM	Approved
TT Robertwood Johnson	Hospital	EHR	manisha.pardeshi@tetruscorp.com	07/24/2020 01:51:28 PM	Pending
TEST TT	Hospital	EMR	vishwajeet8241@gmail.com	03/12/2020 10:56:16 AM	Denied

Heading	Description
<b>HCE Name</b>	The name of the HCE.
<b>Business Type</b>	The business type of the HCE. For example, hospital or pharmacy.
<b>Integration Type</b>	The integration type requested by the HCE. For example, NCPDP.
<b>Email</b>	The business email of the HCE for communication purposes.
<b>Requested Date</b>	The date and time that the HCE integration request was submitted.
<b>Status</b>	The current state of the HCE integration request. For example, <i>Approved</i> , <i>Pending</i> , or <i>Denied</i> .

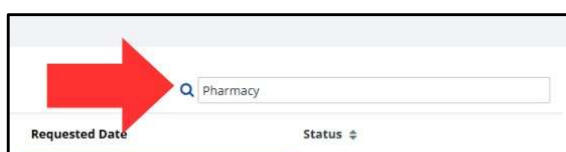
The following subsection contains step-by-step instructions on how to view and search for integration requests in the RxConsole application. For additional clarity, each step is accompanied by a corresponding image or screenshot that depicts the action described.

## 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 that you are searching for by either:
  - Scrolling through the listed requests.
  - 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.

HCE Name	Business Type	Integration Type	Email	Requested Date	Status
ALA	Hospital	NCPDP		12/15/2023 05:19:34 AM	Approved
KXXXXX	Hospital	NCPDP		04/05/2023 06:14:48 AM	Approved
Advent Health	Other			03/30/2023 01:11:55 PM	Pending
BHK	Pharmacy			03/25/2023 01:51:08 AM	Approved
TT_MU2	Hospital	NCPDP		03/20/2023 07:20:01 AM	Approved
TT_MU1	Pharmacy	NCPDP		03/20/2023 07:15:33 AM	Approved
TEST_DG	Hospital	NCPDP		03/01/2023 05:30:14 AM	Pending

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

**Request Form** Back to List

**Status**  
Approved Create HCE

**Healthcare Entity Details**

Name	State	Address
ALA	TT	ddf.adads, CETG (CAS), AL

**Business Details**

Business Type	No. of Facilities	No. of Prescribers
Hospital	121	12

**Email**  
dads@gmail.com

**System Type**  
EHR

**Time frame to connect RxCheck**  
Less than three months

**Integration Type**  
NCPDP

**Contact Details**

Primary Contact	Phone Number	Email
DDD GG	5555555555	ee@g.com

**Secondary Contact**  
No Secondary Contact Details

**Add New Note** Save Note

**Previous Notes (No Notes)**

4. In addition to viewing additional details, you can also perform the following options:
  - a. Create a new HCE 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.

**Request Form** Back to List

**Status**  
Approved Create HCE

**Healthcare Entity Details**

Name	State	Address
ALA	TT	ddf.adads, CETG (CAS), AL

**Business Details**

Business Type	No. of Facilities	No. of Prescribers
Hospital	121	12

**Email**  
dads@gmail.com

**System Type**  
EHR

**Time frame to connect RxCheck**  
Less than three months

**Integration Type**  
NCPDP

**Contact Details**

Primary Contact	Phone Number	Email
DDD GG	5555555555	ee@g.com

**Secondary Contact**  
No Secondary Contact Details

**Add New Note** Save Note

**Previous Notes (No Notes)**

**Annotations:**

- a)** Points to the **Create HCE** button.
- b)** Points to the **Save Note** button.
- c)** Points to the **Back to List** button.

## 13. Approving Interstate Data Sharing for HCEs

This feature enables state PDMP administrators to grant or deny interstate data sharing access to individual 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 an HCE 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.

**Approve Interstate Data Sharing for Healthcare Entities**

**List of PDMP Sites**

Name	Code	Provider Validation
AA	AA	✗
California	CA	✗
Florida	FL	✗
Test Site GG	GG	✓
Test Site KK	KK	✗
Kentucky	KY	✓
<b>QQ</b>	<b>QQ</b>	→ ✓
Test Site TT	TT	✓

**QQ**

Provider Validation ✓

**List of Healthcare Entities**

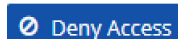
Name	Code	Access	Integration Type	Site Added	Data Sharing
IIR Demo	QQ_IIR	Blocked	EHR	03/28/2025 03:34:48 PM	✓ Grant Access
TEST-TX	QQ_IIR_TX				
QQ_CHE	QQ_CHE	Blocked	HIE	03/12/2025 02:14:39 PM	✓ Grant Access
Advent Health UAT test	QQ_DDD	Blocked	EMR	12/13/2023 04:43:32 PM	✓ Grant Access
NYU	QQ_NYU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

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

Heading	Description
<b>Name</b>	The name of the HCE.
<b>Code</b>	The site code of the HCE.
<b>Access</b>	The access level granted to the HCE by the PDMP state for interstate data sharing.
<b>Integration Type</b>	The integration/site type of the HCE, such as EHR, EMR, HIE, or PDS.
<b>Site Added</b>	The date and time when the HCE was added.



Heading	Description
<b>Data Sharing</b>	The option to grant or deny access to the HCE for interstate data sharing permissions.
<b>Expanded Line—Name</b>	The name of the facility under the selected HCE record.
<b>Expanded Line—Code</b>	The facility code of the facility.
<b>Expanded Line—Email</b>	The email address of the facility for communication purposes.
<b>Expanded Line—Phone</b>	The phone number of the facility.



If an HCE 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 HCEs 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 Data 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-hand side of the screen.

**Note:** QQ has been selected for demonstration purposes.

List of PDMP Sites <input type="text"/>		
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	✓



6. Verify that your action has been successfully implemented by looking for the following alerts:
  - a. If access was granted, an alert that states “Site Unblocked Successfully.”
  - b. If access was revoked, an alert that states “Site Blocked Successfully.”

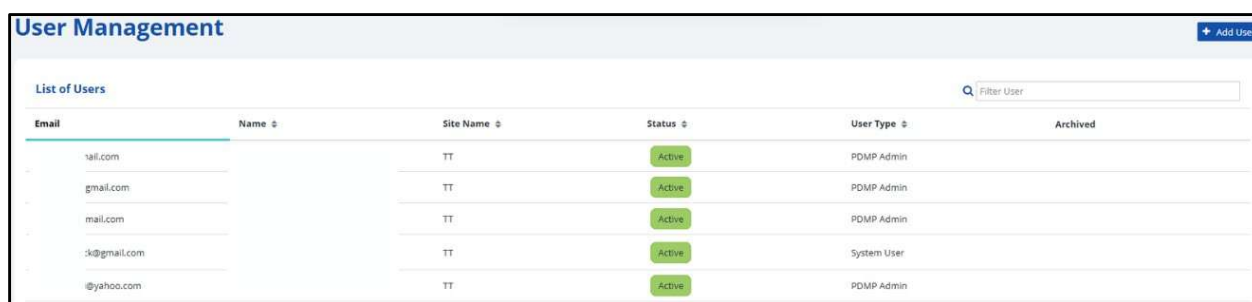


## 14. User Management

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.



The screenshot shows a web interface titled "User Management" with a blue header bar containing an "Add User" button. Below the header is a "List of Users" section with a search bar labeled "Filter User". The main content is a table with columns: Email, Name, Site Name, Status, User Type, and Archived. The table lists five users for site "TT", all with "Active" status. The first three are PDMP Admins, and the last two are System Users.

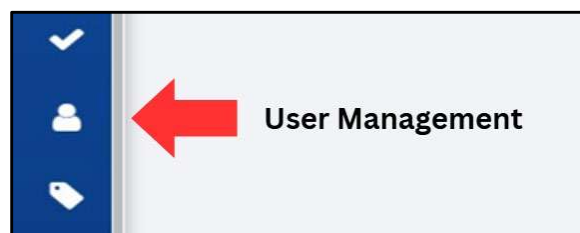
Email	Name	Site Name	Status	User Type	Archived
val.com		TT	Active	PDMP Admin	
gmail.com		TT	Active	PDMP Admin	
mail.com		TT	Active	PDMP Admin	
rk@gmail.com		TT	Active	System User	
@yahoo.com		TT	Active	PDMP Admin	

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 that you are searching for by:
  - a. Scrolling through the list of users displayed on the screen.
  - b. Searching for a user by typing their name into the *Filter User* search bar in the top-right corner of the screen.

**User Management** + Add User

List of Users

Email	Name	Site Name	Status	User Type	Archived
tail.com		TT	Active	PDMP Admin	
gmail.com		TT	Active	PDMP Admin	
mail.com		TT	Active	PDMP Admin	
sk@gmail.com		TT	Active	System User	
@yahoo.com		TT	Active	PDMP Admin	

b)

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 to the RxCheck administrator.

a) **Add/Update User**

Email\*  Password\*  Site Code\*

First Name\*  Middle Name  Last Name\*

Status\* ☒ Active ☐ Inactive Phone Number

b) **Add/Update User**

Contact RxCheck Administrator to update the account

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.

**Add/Update User**

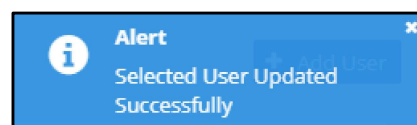
Email\*  Password\*  Site Code\*

First Name\*  Middle Name  Last Name\*

Status\* ☒ Active ☐ Inactive Phone Number

**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
<b>Email</b>	The contact email for the HCE user and username for RxConsole.
<b>Password</b>	The password for the HCE user to access the RxConsole application.
<b>Site Code</b>	The site code for the HCE user. This field will be auto-populated.
<b>First Name</b>	The HCE user's first name.
<b>Middle Name</b>	The HCE user's middle name.
<b>Last Name</b>	The HCE user's last name.
<b>Status</b>	The status of this HCE user's account. Can be set to either active or inactive. A lock icon will be displayed if the account is locked out.
<b>Phone Number</b>	The HCE user's phone number.

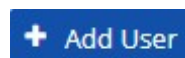
**Note:** See the section titled [User Roles and Privileges in the RxConsole Application](#) for more information about the different user roles available.

## 14.2. Adding Users

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

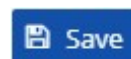


2. Click on the *Add User* button located in the top-right corner of the screen.

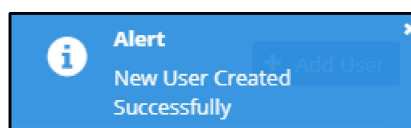


3. In the pop-up window, enter the requested information into the appropriate data field.
  - a. A description of each field is available in the table at the end of the previous section.

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

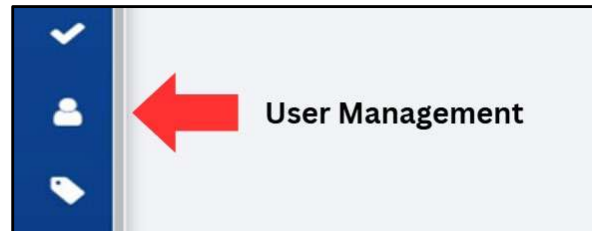


5. Verify that the new user has been successfully added by looking for the alert that states, "New User Created Successfully."



## 14.3. Unlocking a User Account

1. Click on the *User Management* button, located on the left-hand side of the screen.
2. A user account that is locked will display the “lock” icon next to the account status.
3. Click on the lock icon to unlock the account for the corresponding user.
4. Verify that the account has been unlocked by looking for the alert that states, “User Successfully Unlocked.”



## 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 United States are uniquely identified by a 10-digit NPI, issued by the Centers for Medicare and Medicaid Services. Additionally, the DEA in the United States 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 SLN specific to the state in which they practice.

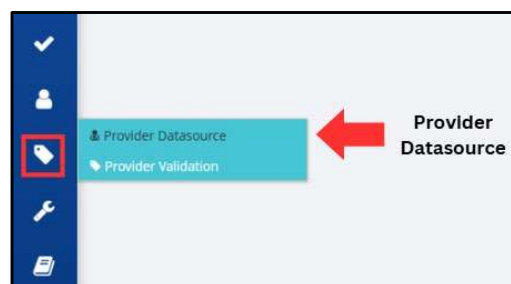
Whenever an HCE sends or receives a prescription data request via RxCheck, the provider’s NPI, DEA, and/or SLN is included in the data payload.

The provider validation feature in RxConsole allows state PDMP administrators to configure whether the validation of the NPI, DEA, SLN and/or other number is required, optional, or not validated prior to processing a request.

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.

Datasources						<a href="#">+ Add Datasource</a>
List of Datasources						<input type="text" value="Global Filter"/>
Datasource Name	Datasource Type	API URL	Auth Type	Records	Created Date	
MTESTTT	FILE			14	11/05/2025 05:02:07 PM	
ffdafa	FILE				07/29/2025 11:51:53 PM	
Testdatasource2	FILE				05/08/2025 11:36:58 AM	
Testdatasource	FILE				05/08/2025 11:35:37 AM	



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*.

A screenshot of a web interface titled "List of Datasources". It features two columns: "Datasource Name" and "Datasource Type". The first row shows "Testdatasource2" under the name column and "FILE" under the type column. The second row shows "Testdatasource" under the name column and "FILE" under the type column. A red arrow points to the "Testdatasource2" text in the first row.

Datasource Name ↕	Datasource Type ↕
Testdatasource2	FILE
Testdatasource	FILE

Header	Description
<b>Datasource Name</b>	The name entered by the PDMP administrator referencing this unique datasource.
<b>Datasource Type</b>	Identifies the datasource type as a file or API.
<b>API URL</b>	The URL for the API to call for provider identification.
<b>Auth Type</b>	The authorization method for calling the API.
<b>Records</b>	The number of records on the datasource in this row.
<b>Created Date</b>	The date and time that the datasource was added into the RxConsole.

## 15.2. View, 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*.

**Datasource**

Datasource Name: MTESITT Datasource Type: FILE

**Data Upload**

Manage File Search Provider

Search Provider Records Count: 14 | Upload Timestamp: 11/05/2025 05:04:53 PM

DEA# NPI# SL# OTHER#

Enter DEA# Enter NPI# Enter SL# Enter OTHER#

Preview Sample Records Search

2. To see if an existing datasource file contains a provider, you can enter the DEA, NPI, SLN, or other number in the *Search Provider* section to see if that provider exists on the datasource that 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)

DEA# NPI#

MDEA10302025 Enter NPI#

Found 2 record(s)

First Name	Last Name	DEA#
		MDEA10302025
		MDEA10302025

b)

Search Provider

Records Count: 6 Upload Timestamp: 05/08/2025 11:42:02 AM

DEA# NPI# SL#

Enter DEA# Enter NPI# 15487

No Provider found.

Search

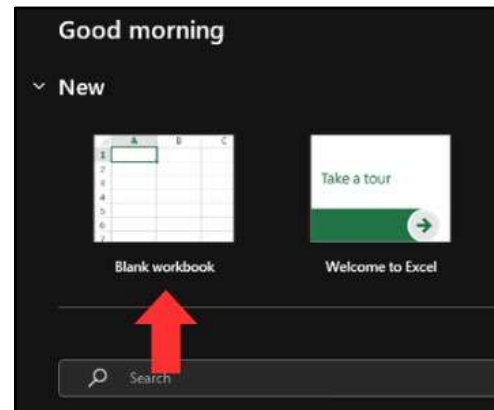
**Note:** The datasource search feature is only available for datasource files and cannot be used on a datasource API.

### 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 that you would prefer. The names of the possible headers are:
  - First Name
  - Last Name
  - NPI#
  - DEA#
  - SL#
  - OTHER#

**Note:** The header names should be entered in cells A1, B1, C1, D1, E1, and F1.

A screenshot of an Excel spreadsheet showing the first six columns (A-F) and the first six rows (1-6). The headers are: A1: First Name, B1: Last Name, C1: NPI#, D1: DEA#, E1: SL#, F1: OTHER#. The rest of the cells are empty.

	A	B	C	D	E	F
1	First Name	Last Name	NPI#	DEA#	SL#	OTHER#
2						
3						
4						
5						
6						

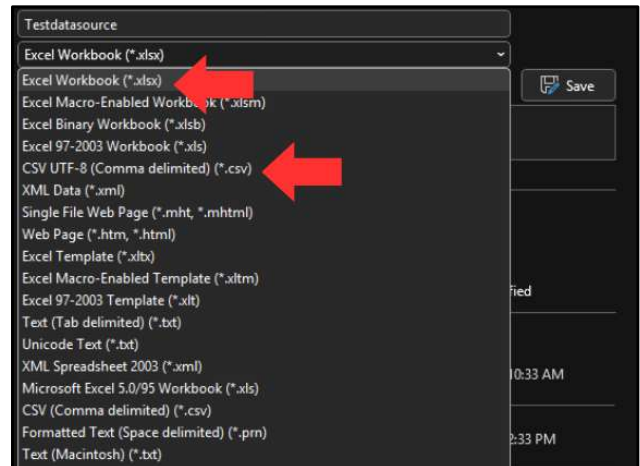
**Note:** Not all header names are required, and any combination of headers can be used (e.g., if a state administrator does not want to use the DEA number, they may elect to remove that header completely).

- 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

- When finished building your datasource file, save the file as either a .csv or .xlsx (Excel workbook).



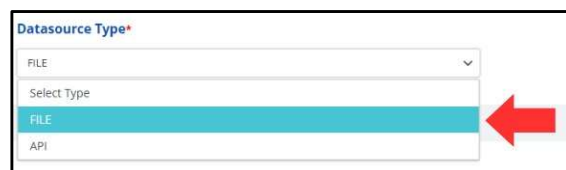
### 15.2.2. Add a New Datasource File

- Follow steps one through three under the section titled [View and Add a Datasource for Provider Validation](#) in this guide.
- Select the “File” option under the *Datasource Type* drop-down.

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

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

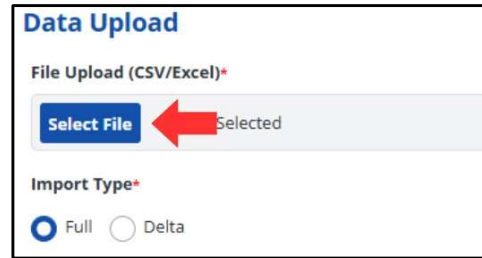
**Note:** The name does not need to match your datasource file. The name in this field can be up to 15 alphanumeric characters (spaces and special characters are not allowed).



### Datasource

**Datasource Name\***

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



**Data Upload**

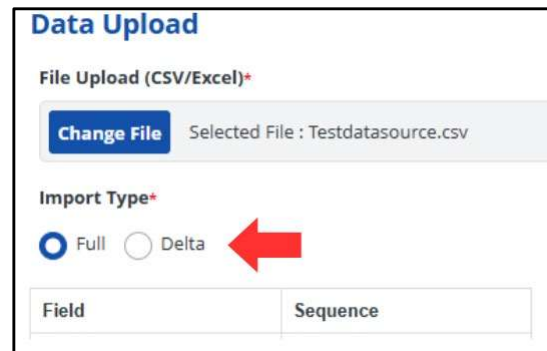
File Upload (CSV/Excel)\*

**Select File** Selected

Import Type\*

☒ Full ☐ Delta

5. Select your import type:
  - a. Full: Will import the entire datasource file under the name that you entered in step three.
  - b. Delta: This is only available when viewing a previous datasource (see previous section titled [View and Add a Datasource for Provider Validation](#) for instructions to view a previous datasource).



**Data Upload**

File Upload (CSV/Excel)\*

**Change File** Selected File : Testdatasource.csv

Import Type\*

☒ Full ☐ Delta

Field	Sequence

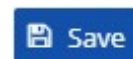
6. Check the fields that are present in your datasource file. If you did not include a field, you can leave the box unchecked.
  - a. After checking the box, you will need to set the sequence. This refers to the order of the columns in your datasource file.

**Note:** Column A is sequence “0,” Column B is sequence “1,” etc.

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

Field	Sequence
<input checked="" type="checkbox"/> First Name	<input type="text" value="1"/>
<input checked="" type="checkbox"/> Last Name	<input type="text" value="0"/>
<input checked="" type="checkbox"/> NPI#	<input type="text" value="4"/>
<input checked="" type="checkbox"/> DEA#	<input type="text" value="2"/>
<input checked="" type="checkbox"/> SL#	<input type="text" value="3"/>
<input checked="" type="checkbox"/> OTHER#	<input type="text" value="5"/>

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

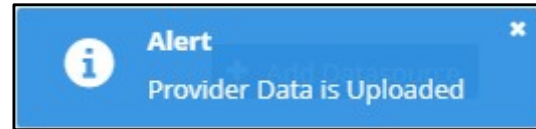


- Alternatively, if you do not wish to add your datasource, you can press the *Cancel* button to discard changes and return to the previous screen.



- Verify that 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*.



List of Datasources	
Datasource Name ↕	Datasource Type ↕
Testdatasource2	FILE
Testdatasource	FILE

### 15.2.3. Add a Datasource API

- Follow steps one through three under the section titled [View and Add a Datasource for Provider Validation](#) in this guide.
- Select the “API” option under the *Datasource Type* drop-down.
- Enter the API URL into the field labeled *API URL*.
- Select the appropriate authorization type using the *Auth Type* drop-down.
- For BASIC authorization, enter the username and password.

The screenshot shows three parts of a form. The top part is a 'Datasource Type' dropdown menu with 'API' selected and highlighted in blue, indicated by a red arrow. The middle part is 'API Datasource Validation' with an 'API URL' field containing the placeholder text 'Enter API URL'. The bottom part is an 'Auth Type' dropdown menu with 'BASIC' selected and highlighted in blue.

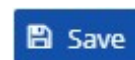
### API Datasource Validation

<b>API URL*</b>	<b>Auth Type*</b>
<input type="text" value="https://npiregistry.cms.hhs.gov/api/?version=2.1"/>	<input type="text" value="BASIC"/>
<b>Username*</b>	<b>Password*</b>
<input type="text" value="Enter Username"/>	<input type="text" value="Enter Password"/>

- For OAUTH2 authorization, enter the client ID, client secret, and auth URL into their respective fields.

<b>API URL*</b>	<b>Auth Type*</b>
<input type="text" value="https://npiregistry.cms.hhs.gov/api/?version=2.1"/>	<input type="text" value="OAUTH2"/>
<b>Client ID*</b>	<b>Client Secret*</b>
<input type="text" value="Enter Client Id"/>	<input type="text" value="Enter Client Secret"/>
<b>Auth URL*</b>	
<input type="text" value="Enter Auth URL"/>	

- Press the *Save* button on the right corner of the screen to add your datasource API to the RxConsole for your state.
- 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.
- Verify that the datasource API was successfully added by looking for the alert that states, "Datasource Created."



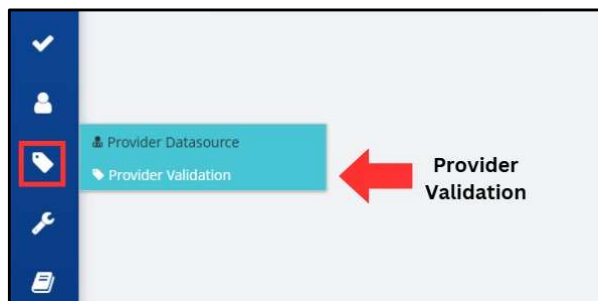
You will also return to the Datasource screen and should see your datasource in the *List of Datasources*.



## 15.3. Configure Provider Validation Options

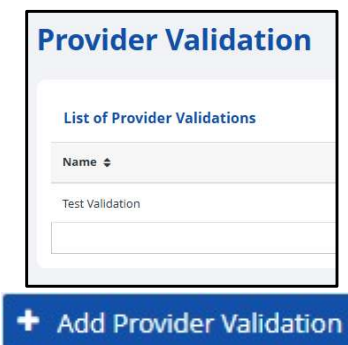
### 15.3.1. Modify an Existing Provider Validation

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

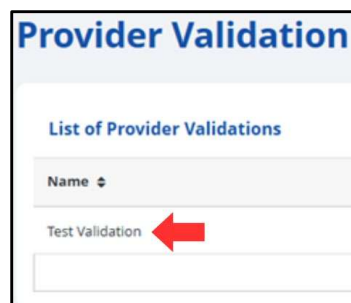


2. The Provider Validation screen allows you to view a list of existing validations that have been added and includes a button to add a new provider validation.

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




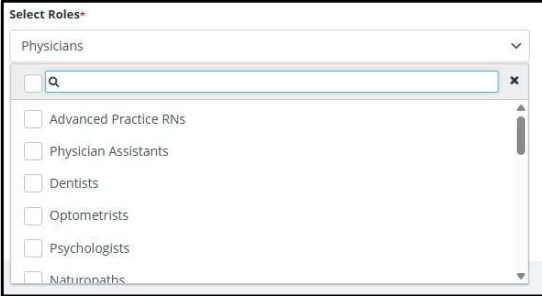
3. To view and/or modify an existing validation, click on the name of a validation.








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.

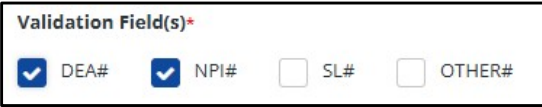
a) 

b) 

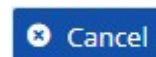
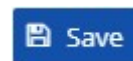
c) 

d) 

e) 

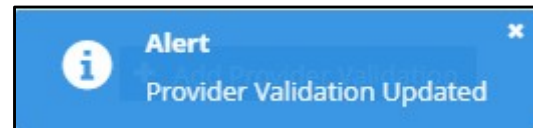
f) 

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



- Verify that the provider validation was successfully updated by looking for the alert that states, "Provider Validation Updated."

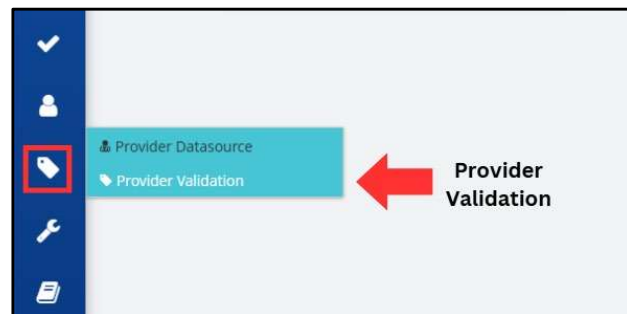
You will also return to the provider validation screen and should see your changes in the *List of Provider Validations*.



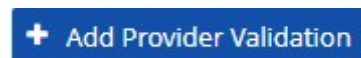
Header	Description
<b>Name</b>	The name given to this specific set of validation rules.
<b>Datasource Name</b>	The name of the datasource that is referenced for validation.
<b>Validation Fields</b>	The identification numbers that are subject to validation.
<b>Validate Type</b>	With the type of validation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

### 15.3.2. Add a New Provider Validation


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

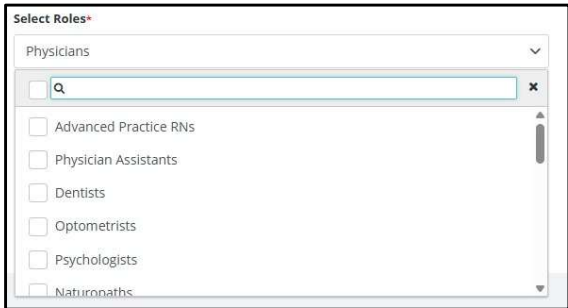



- To add a new set of validation rules, click on the *Add Provider Validation* button.





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 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.


a) 

b) 

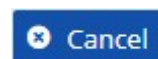
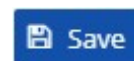
c) 

d) 

e) 

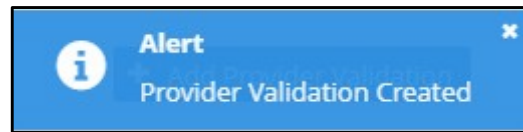
f) 

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 that 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*.

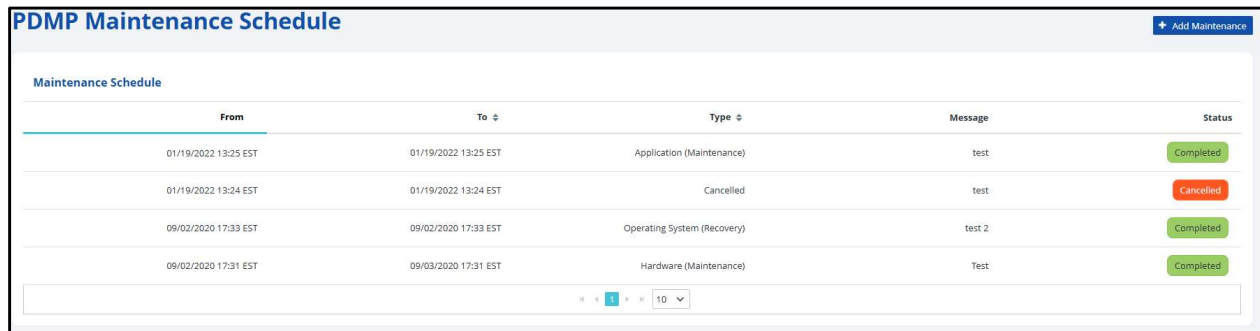


## 16. PDMP Maintenance Schedule

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.



From	To	Type	Message	Status
01/19/2022 13:25 EST	01/19/2022 13:25 EST	Application (Maintenance)	test	Completed
01/19/2022 13:24 EST	01/19/2022 13:24 EST	Cancelled	test	Cancelled
09/02/2020 17:33 EST	09/02/2020 17:33 EST	Operating System (Recovery)	test 2	Completed
09/02/2020 17:31 EST	09/03/2020 17:31 EST	Hardware (Maintenance)	Test	Completed

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

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

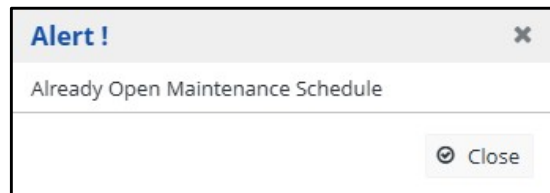
1. Click on the *PDMP Maintenance Schedule* button, located on the left-hand side of the screen.



2. Click on the *Add Maintenance* button located on the top-right 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.

A screenshot of a "Maintenance" pop-up window. The window has a title bar with "Maintenance" and a close icon. Inside, there are three fields: "From Date&Time\*" with a calendar icon, "To Date&Time\*" with a calendar icon, and "Reason Type\*" with a dropdown menu showing "Not Selected". Below these is a small note: "\*\*Date Time is EST Timezone". Underneath is a large text area labeled "Reason Message\*". At the bottom right are two buttons: "Save" and "Close".

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*.

The screenshot shows the 'From Date&Time' field with a blue calendar icon. A red arrow points to this icon. Below the field, a calendar for May 2025 is displayed, showing dates from 27 to 31. The time is set to 14:20.

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*.

The screenshot shows the 'To Date&Time' field with a blue calendar icon. A red arrow points to this icon. Below the field, a calendar for May 2025 is displayed, showing dates from 27 to 31. The time is set to 14:22.

6. Select the reason for the maintenance event by clicking on one of the drop-down options for the field labeled *Reason Type*.

The screenshot shows the 'Reason Type' field with a dropdown menu. The options are: Not Selected, Application (Installation), Application (Maintenance), Hardware (Installation), Hardware (Maintenance), and Operating System (Reconfiguration).

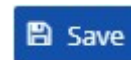
7. Add a note into the text box labeled *Reason Message* to add context to the maintenance event.

Reason Message\*

Updating the server

Save Close

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:

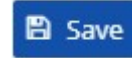
10. Click on an event listed in the *Maintenance Schedule*.

From	To	Type	Message	Status
05/09/2025 14:08 EST	05/09/2025 14:08 EST	Cancelled	Change	Cancelled
01/19/2022 13:25 EST	01/19/2022 13:25 EST	Application (Maintenance)	test	Completed
01/19/2022 13:24 EST	01/19/2022 13:24 EST	Cancelled	test	Cancelled
06/02/2020 17:33 EST	06/02/2020 17:33 EST	Operating System (Recovery)	test 2	Completed
06/02/2020 17:31 EST	06/02/2020 17:31 EST	Hardware (Maintenance)	Test	Completed



11. Modify any information in the *Maintenance* pop-up, 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 that they offer. These codes are assigned at both the individual and organization provider levels and 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 five 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		
367S00000X	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
<b>Taxonomy Code</b>	Administrative codes set for identifying the provider type and area of specialization for healthcare providers.  They consist of 10 alphanumeric characters always ending with the letter "X."
<b>Description</b>	A brief description of the healthcare professional role displayed for that taxonomy code.
<b>PMIX Role</b>	The PMIX role that the corresponding taxonomy code is mapped to.
<b>PDMP</b>	The PDMP state for which the taxonomy code was created.
<b>Source</b>	Defines the origin of the taxonomy code.

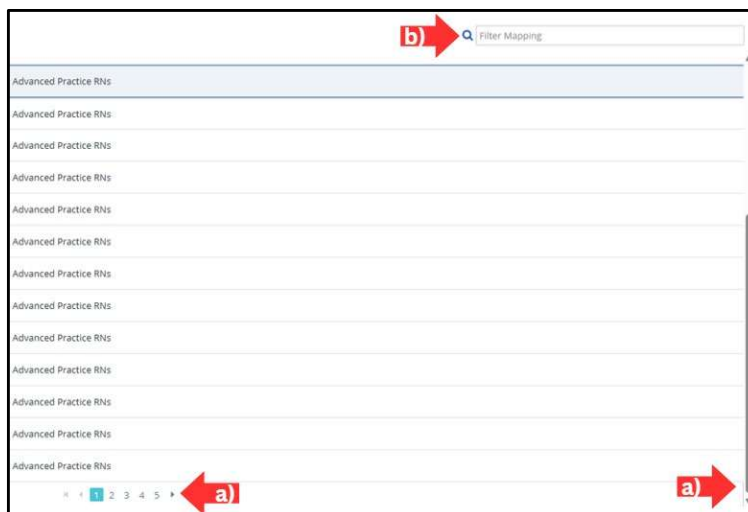
The following section contains step-by-step instructions on how to search for an NCPDP code in the RxConsole application. For additional clarity, each step is accompanied by a corresponding image or screenshot that depicts the action described.

## 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.



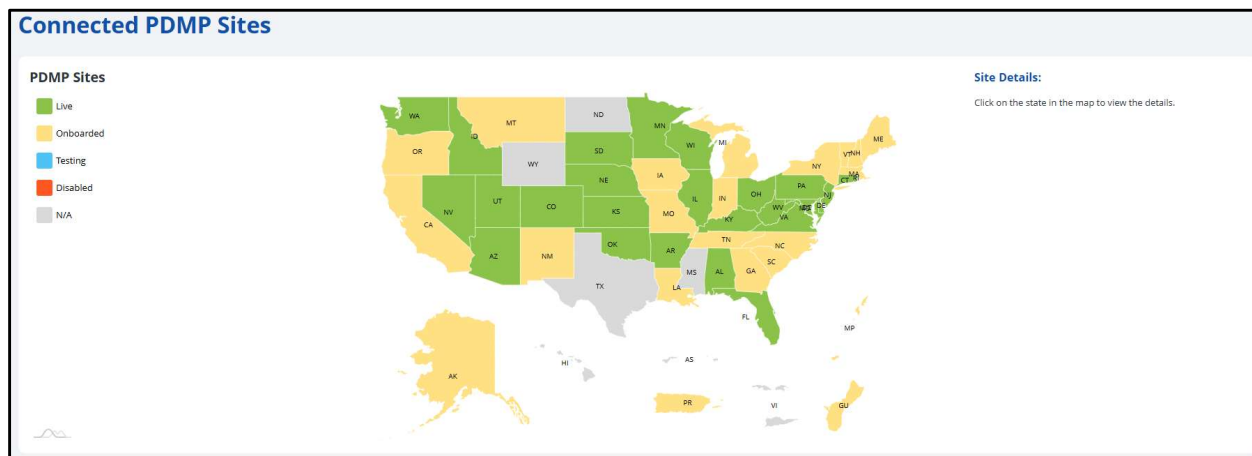
2. Locate the code mapping that you are searching for by either:
  - a. Scrolling through the list of codes displayed on the screen and sifting through the pages by clicking the arrows under the *Code Mapping* table.
  - b. Locate the mapping directly by entering the taxonomy code, description, or PMIX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



## 18. System Information

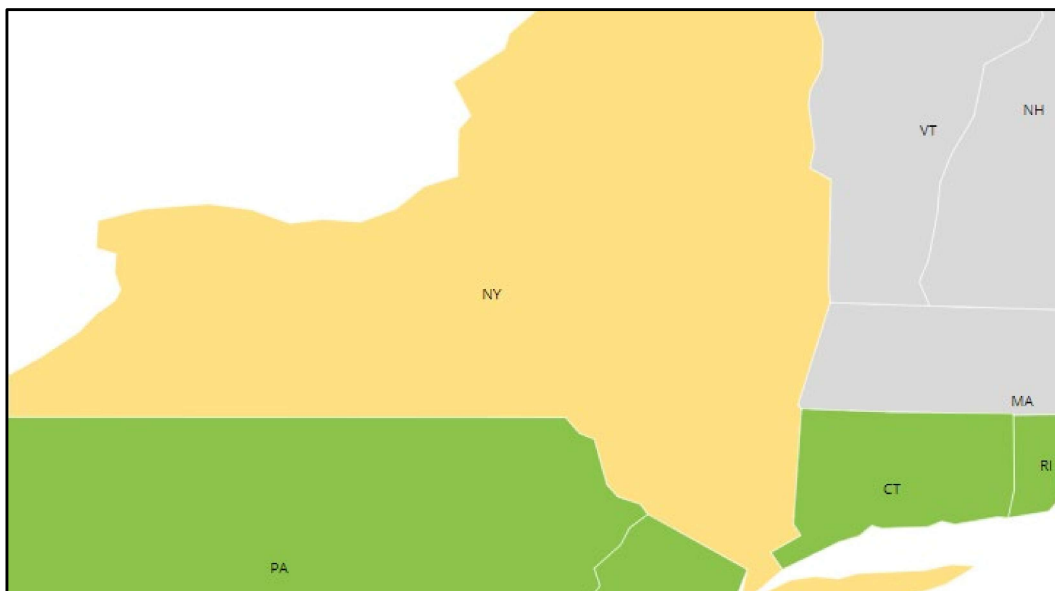
The System Information feature presents a graphical map of the United States, illustrating the deployment and connection status of each state within the RxCheck network.

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.

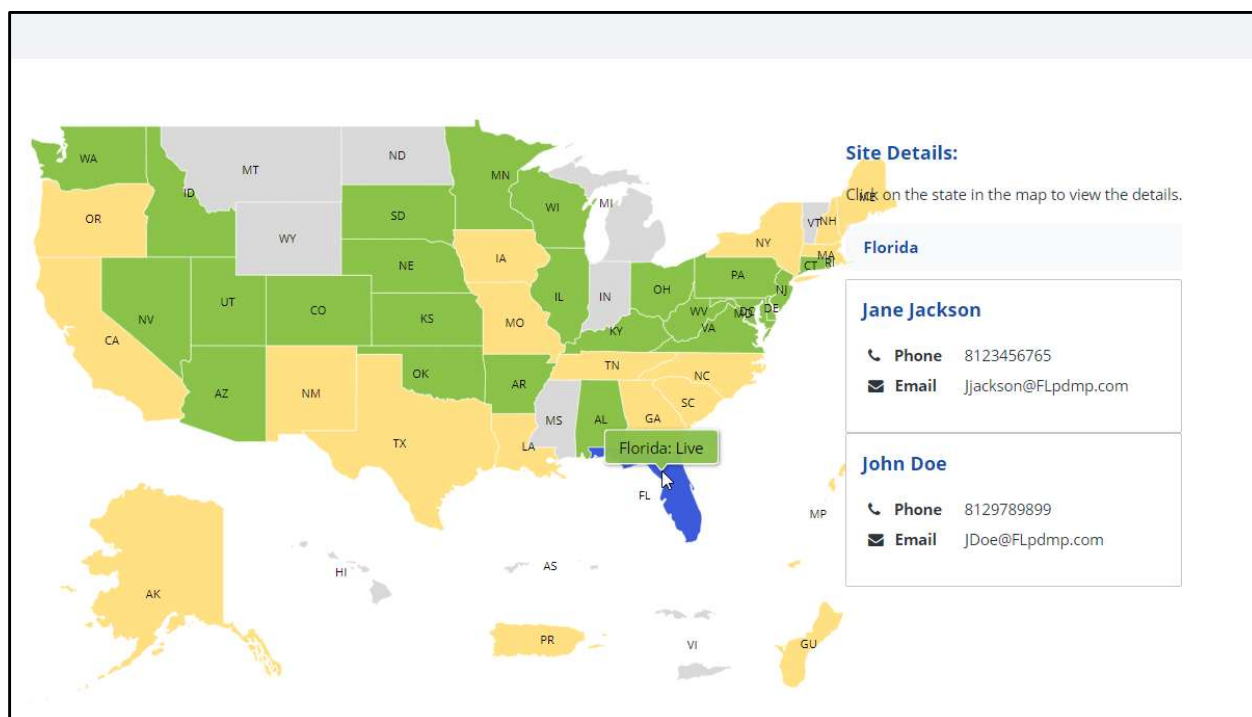


Status	Color Code	Color
Live	Green	
Onboarded	Yellow	
Testing (or Hovering)	Blue	
Disabled	Orange	
N/A	Gray	

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.



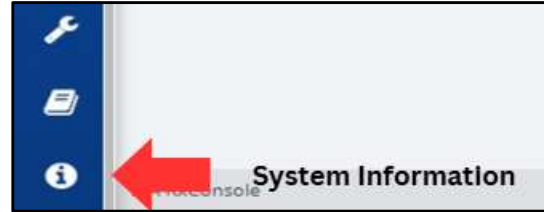
Clicking on each state will also display additional site details, such as the phone and email address of the point-of-contact person for that state, as seen in the diagram below.



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.

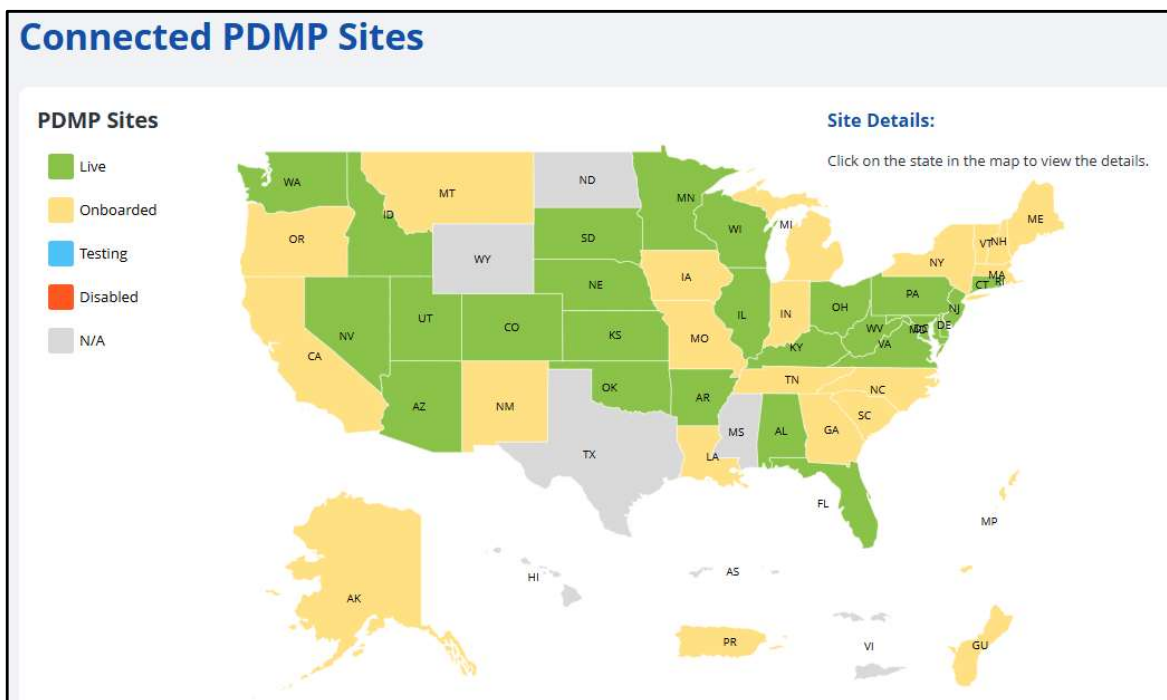
## 18.1. Connected PDMP Sites

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

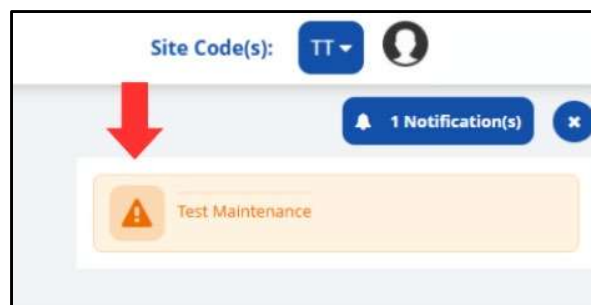
In addition to Heartbeat Notifications, RxConsole offers system notifications within the application. These applications are designed to remind or notify users of important information.

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.

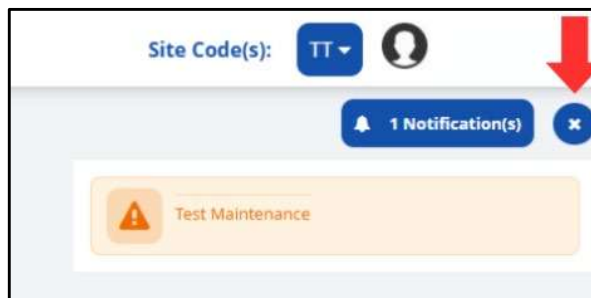


2. Clicking on the *Notification(s)* icon will display the message relating to the notification, if a notification exists.

**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.

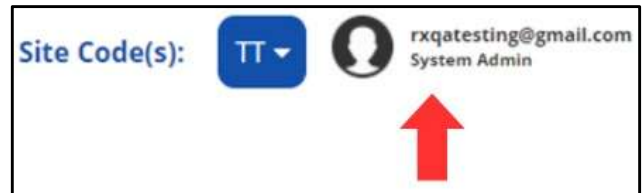


Notifications will be shown for:

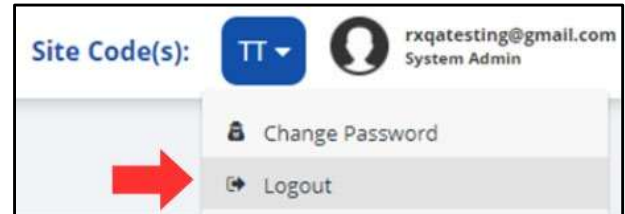
- Heartbeat Notifications
- New MOU Worksheets
- Scheduled Maintenance Events
- Certificate Expirations
- Release Updates

## 20. Exit the RxConsole Application

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



2. Select the *Logout* drop-down option.





## 21. Contact the RxCheck Team

To connect with the RxCheck team, visit the RxCheck website at [www.rx-check.org](http://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](http://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	
3.2	IJIS Institute	12-2025	Updated HCE registration to include vendor connect features, Hub Audit Log/provider validation to include <i>OTHER#</i> , and added section for unlocking user accounts.

*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 [pdmpptac@iir.com](mailto:pdmpptac@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](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](https://en.wikipedia.org/wiki/National_Council_for_Prescription_Drug_Programs)
6. <https://www.hl7.org/implement/standards/>
7. <https://nascsa.org/pmix-standards/>