BioSense Platform User Manual for the Access & Management Center

September 2023

Centers for Disease Control and Prevention
Office of Public Health Data, Surveillance, and Technology

Technical Assistance: support.syndromicsurveillance.org

The National Syndromic Surveillance Program (NSSP) promotes the use of automated, electronic health data. NSSP provides a secure and integrated electronic health information system that hosts standardized analytic tools and facilitates collaborative processes. The NSSP is a product of the Centers for Disease Prevention and Control (CDC).

BioSense Platform User Manual for the Access & Management Center

September 2023

Produced by

Office of Public Health Data, Surveillance, and Technology
Centers for Disease Control and Prevention

Revision History

Date	Revisions
September 2023	▪ Updates reflect enhancements and changes in User Interface and functionality between release 1.6.3 and release 1.8.0
August 2022	▪ Updates reflect enhancements and changes in User Interface between release 1.5.4 and release 1.6.3 (**Sections 2–5 and 7–11)**
April 2021	▪ Updates reflect enhancements and changes in User Interface, release 1.5.4 (**Sections 2–5, 7, and 9)**
November 2020	▪ Removes references to the Adminer tool that has been retired
September 2020	▪ Supports AMC software release 1.5.3 ▪ Describes new rules for managing and restricting data access (Section 5.1.8, "Selecting Clinical Laboratory Data") (Section 5.1.9, "Selecting Mortality Data") ▪ Describes enhancements to the Master Facility Table (Section 9.1, "Facilities Inactivation Reason and Date") (Section 9.2, "Facilities in U.S. Territories")
July 2020	▪ Supports AMC software release 1.5.2 ▪ Converts Quick Start Guide to User Manual ▪ Describes new rules for managing (and restricting) data access (Section 5.1.7, "Selecting Syndromic Restrictions") ▪ Describes enhancements to Reports Tab (Section 10, "Reports")

Contents

1. Overview

The Access & Management Center (AMC) provides a common access point for NSSP applications and supports the BioSense Platform's administrative functions for implementing tools and applications.

Users have access to the AMC Home tab's three sections:

- *My Info* section provides access to the user's profile information (My Profile), a Change Password function, and a copy of the Users Code of Conduct.
- The *NSSP Application* section provides links to ESSENCE, data query and analysis tools, and Data Quality Dashboard.
- The *Resources* section provides links to the Service Desk, Data Dictionary, and other resources.

For those with elevated privileges, such as site administrators, the AMC provides functionality in multiple tabs. In addition to the Home tab that everyone sees, the following tabs provide administrative and access functionality:

- The Manage Users tab allows site administrators to modify information for any of their site's users. Site administrators can control user access to the ESSENCE National View and Chief Complaint Query Validation Tool. Access to the DataMart, Posit (RStudio) Workbench, and SAS Studio can be granted here. Platform-wide communications (Data Quality and Processing and Onboarding Communications) is also granted from this tab.
- The Data Access tab provides an interface to existing rules that control access to ESSENCE data on an individual or group level. Here existing rules can be modified or deleted, and new rules can be created. Data access rules allow site administrators to control access to the site's Data Sources for everyone who uses the Posit (RStudio) Workbench and SAS Studio applications.
- The User Groups tab displays the user groups edit page. Existing groups can be renamed, and members can be added or deleted. User Groups can be designated as Public (viewable by all sites) or Private (only viewable within the site).

What is a site?

NSSP organizes facilities (e.g., hospitals, emergency departments, urgent care centers) under a single *administrative authority* called a *site*. A site may oversee any number of facilities, all of which share the same site administrator and Master Facility Table (facility metadata).

What is a site administrator?

- A site administrator creates user accounts and controls access to data on the BioSense Platform.
- Your site will assign one or more people to serve as site administrator.

If you're a site administrator and need access to the AMC, please submit a ticket to the NSSP Service Desk at NSSP Service Desk.

What is Posit?

RStudio has been shifting from an R language-centric Integrated Development Environment (IDE) to become more language neutral. For now, Python language is providing more functionality and has opened RStudio to provide more flexibility. Of course, R language is still supported.

To better reflect this shift to open RStudio using more languages, the company has chosen to rebrand to the name **Posit**. So RStudio or Posit, it's still the same IDE you are used to. It just has a new name.

During this time of transition, you may see references to RStudio Workbench and Posit Workbench. They both refer to the Workbench IDE you are used to using.

2. Access

2.1 Obtaining Log-in Credentials

To request AMC access, contact the site administrator(s) for your site. Sites are responsible for creating policies to manage user accounts and access to your data. If you are the site administrator, contact the NSSP Service Desk at https://support.syndromicsurveillance.org and open a request ticket.

What happens when my account is created in the AMC?

- You will receive two emails from amc@syndromicsurveillance.org. One will contain your new username and the other email will have your one-time password. You must log in to the AMC to accept the Code of Conduct and set a new password before logging in to ESSENCE or other applications.
- This new username will work for all applications on the BioSense Platform to which you have access, including AMC, ESSENCE, Posit (RStudio) Workbench, and SAS Studio. Not all users have access to all applications on the BioSense Platform.

2.2 Logging In to AMC

1. Go to https://amc.syndromicsurveillance.org/.
2. Enter the username and temporary password sent to you via separate emails (Figure 1).
3. Click **Submit**.

Figure 1. AMC Log-in Screen

If you forget your password or username, you can use the links on this login page to retrieve them. If you believe your credentials are correct but still have trouble logging in to the AMC, contact the NSSP Service Desk at http://support.syndromicsurveillance.org.

2.3 Review and Accept Code of Conduct

The first time you log in to the system, you are required to review and accept the BioSense Platform Code of Conduct shown in Figure 2. The Code of Conduct outlines proper practices and responsibilities (data-sharing etiquette) for the BioSense Platform user community.

Users must accept the Code of Conduct under the following conditions:

- First time logging in
- Every 90 days when password expires
- When user resets password
- When changes are made to user's authorized access (for example, if a user account becomes a site administrator account)

You must read the Code of Conduct. When you reach the end, the **I Agree** button will illuminate. If the button doesn't activate after reading the entire Code of Conduct, we suggest reducing the zoom on your browser from 100% to 80% or 90% in your browser settings.

2.4 Activating Your Account

You must change your password the first time you log in to the AMC, as shown in Figure 3. You will not be able to access the AMC or other tools until you agree (see red arrow) to the BioSense Platform Code of Conduct and change your password. **Note:** You must read the Code of Conduct while scrolling all the way to the end before the "I Agree" button will activate. Click **I Agree**.

The first time you log in, your "Old Password" will be the one-time password you received in the email from amc@syndromicsurveillance.org. *This email account is not monitored. Do not send or reply to this email address.*

When creating a new password, be aware that all passwords must meet the following minimum requirements:

Figure 2. BioSense Platform Code of Conduct

Password Requirements for Site Administrators

- Passwords must meet these four criteria:
  - Contain both upper and lowercase letters
  - Contain numbers
  - Contain special characters
  - Contain *exactly* 12 characters
- Passwords must *not* contain a sequence of three or more characters from any part of the following:
  - First name
  - Last name
  - Email address
  - The word "password"
- Passwords must be more than 75% different from your previous password on a character-by-character basis. For example, ABCD is original password, AEFG or ADBC are valid changes, but AECD or ABCE are invalid changes).
- AMC keeps a history of previous passwords, so your new password must not match any of your previous 24 passwords.

- Because there are specific password requirements, we recommend using a random password generator for enhanced security. Search the internet for "Free Password Generator" to find links to various utilities that are available to do this.
- You may change your password at any time but are *required* to change it every 90 days. **The same username and password combination is used for AMC, ESSENCE, Posit** (RStudio) **Workbench, and SAS Studio.**
  Note: This is accomplished with the Windows Active Directory (AD) functionality, so when you change your password, there might be a delay from 5 to 45 minutes while your password change propagates through the AD system. Please be patient.
- First-time users should be made aware of the AD propagation delay. When you change your password, you may not be able to log in to ESSENCE, Posit (RStudio) Workbench, and SAS Studio immediately. Please wait at least 5 minutes before trying.

You cannot log in to any NSSP applications until you have accepted the Code of Conduct and reset your initial password in the AMC.

Here is what the Change Password screen looks like (Figure 3):

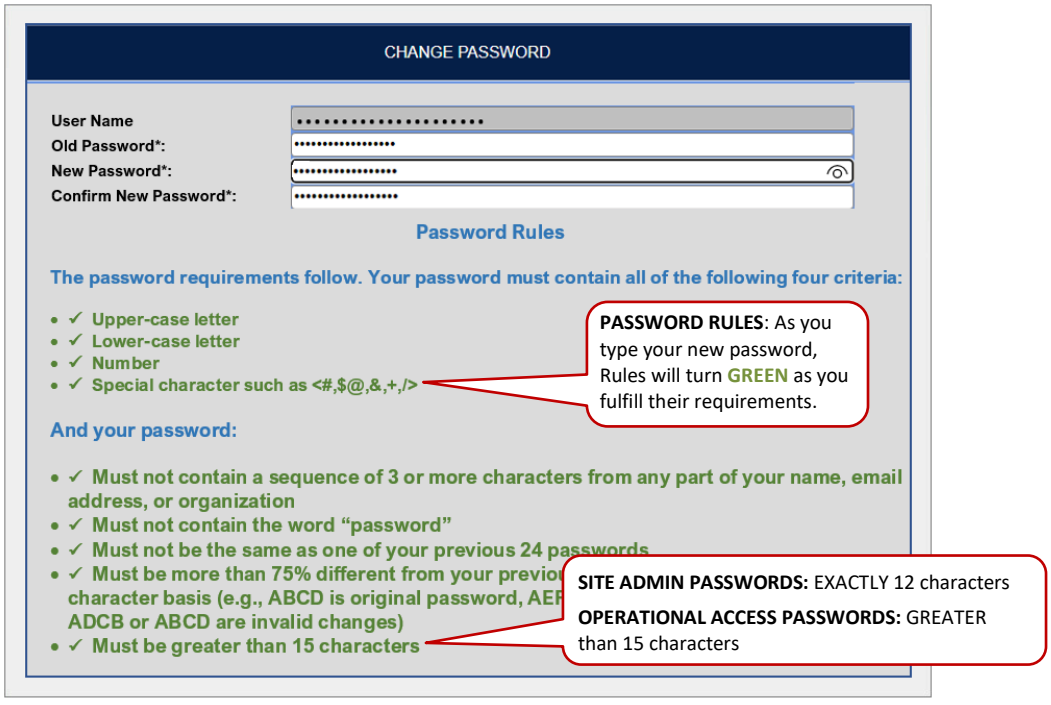


Figure 3. Change Password Screen with Dynamic Rule Validation

When you begin typing in your new password, it is dynamically checked against the required rules. In the example below (Figure 4), we started typing a new password to illustrate how this works.

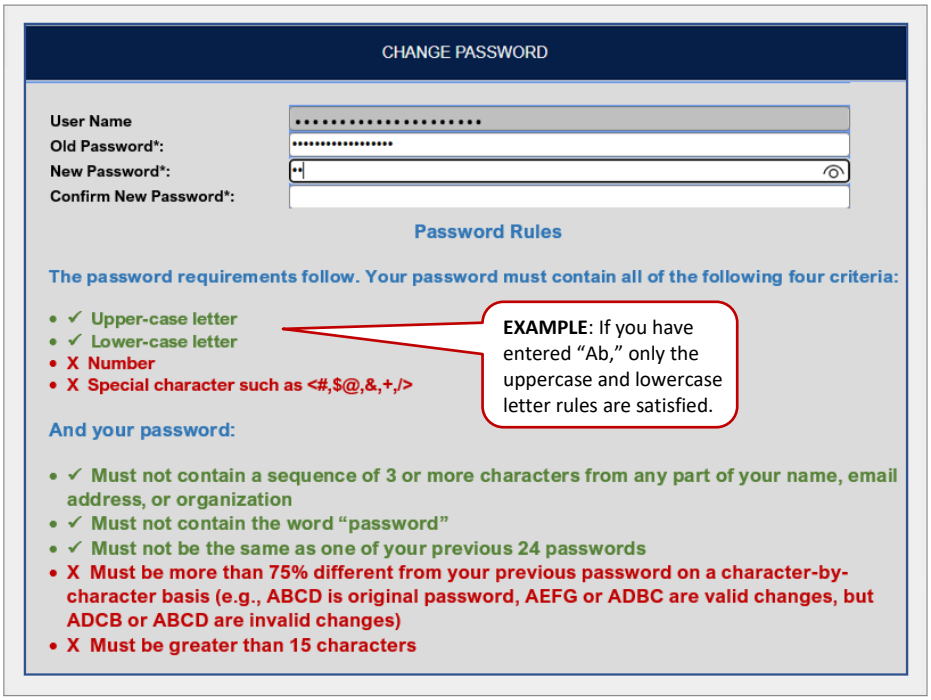


Figure 4. Dynamic Password Rule Check

What if I forget my password?

Navigate to the AMC log-in page and click **Forgot Password?**

Provide the requested information to receive an email with a new one-time password:

- When you receive your new password, use it to log in to AMC.
- Once logged in, you will be taken directly to the BioSense Platform Code of Conduct screen to read the Code of Conduct and click the **I Agree** button before proceeding.
- Once you agree to the BioSense Platform Code of Conduct, you will be taken directly to the Change Password screen and required to change your password.
- Enter your one-time password as your "Old Password," and follow the password requirements on the Change Password screen to create a new password.

3. Home Page

3.1 Users Home Page

Information about the AMC home page for users (Figure 5) is provided here for reference. This screen allows regular users to access their My Info pane, which provides them with their user profile information, change password functionality, and a copy of their Code of Conduct, and to their NSSP Applications pane. In addition, the Resources pane displays links to useful resources. They are briefly explained below in Figure 5.

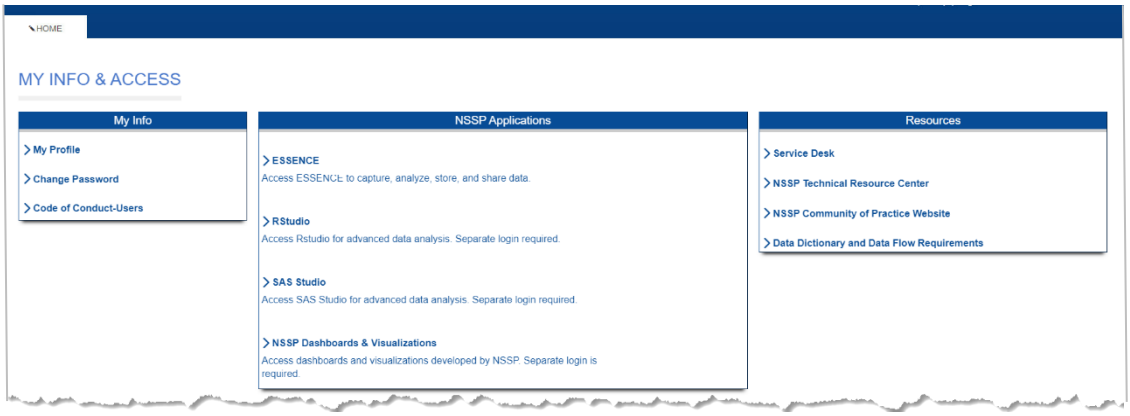


Figure 5. AMC User Home Page

My Info

Users can follow links to change their password, update selected profile data (name, email address, phone number, and organization), and view the "Code of Conduct – Users" that is required for accessing the BioSense Platform's AMC tool.

NSSP Applications

Users and site administrators can gain quick access to tools and applications for viewing data submitted to the BioSense Platform:

- ***ESSENCE***—Capture, analyze, store, and share data
- ***Posit*** (RStudio) ***Workbench***—View MS SQL data and perform advanced data analysis
- ***SAS Studio***—View MS SQL data and perform advanced data analysis
- ***NSSP Dashboards and Visualizations***—Review data processing and data quality for your site

Resources

- ***NSSP Service Desk***—You will be asked to set up a password. Once you have a password, you may submit general or technical questions about NSSP. Your question will be routed to a specialist. Link: **Service Desk.**
- ***NSSP Technical Resource Center***—This is a go-to place for NSSP publications (user manuals, quick start guides), forms, standards and guidance, message mapping guides, fact sheets, onboarding guidance and job aids, and access to BioSense Platform applications. Link: **Technical Resource Center.**
- ***NSSP Community of Practice Website***—The website links to forums, work groups, training, Knowledge Repository, and more. This website is for anyone interested in syndromic surveillance who wants to collaborate, share ideas, and learn from or contribute to the community. Link: **NSSP Community of Practice.** (**Note:** The Council of State and Territorial Epidemiologists [CSTE] facilitates the NSSP Community of Practice through a cooperative agreement with CDC.)

- ***Data Dictionary and Data Flow Requirements***—The Data Dictionary promotes standards-based vocabulary for exchanging consistent information among public health partners. The Dictionary contains details on data elements stored in NSSP data tables. Worksheets link to the Public Health Information Network Vocabulary Access and Distribution System (PHIN VADS) website for specific data elements associated with a standard. Link: **NSSP Data Dictionary Spreadsheet.**

3.2 Site Administrator Home Page

Site administrators can perform additional functions in the AMC. The home page for site administrators (Figure 6) includes the following tabs:

- ***Home***—Update profile, change password, navigate to BioSense Platform applications, and resources.
- ***Manage Users***—Add, modify, or inactivate user accounts for your site.
- ***Data Access***—Add, modify, or remove data access permissions for ESSENCE accounts.
- ***User Groups***—Add, modify, or remove groups and group members.
- ***Master Facility Table (MFT)***—Add, modify, or view facilities for your site, including adding and editing multiple primary facilities. Allows site administrators and users with MFT_Edit_User privileges to review and approve pending facility changes.
- ***MFT Review***—Available to operational access users (also called superusers) as part of the onboarding process.
- ***Reports***—View users who can access your data.
- ***Admin***—Site administrators can view Software Usage metrics for their site's Posit (RStudio) licensees. Other applications may be added to this tab in future releases.

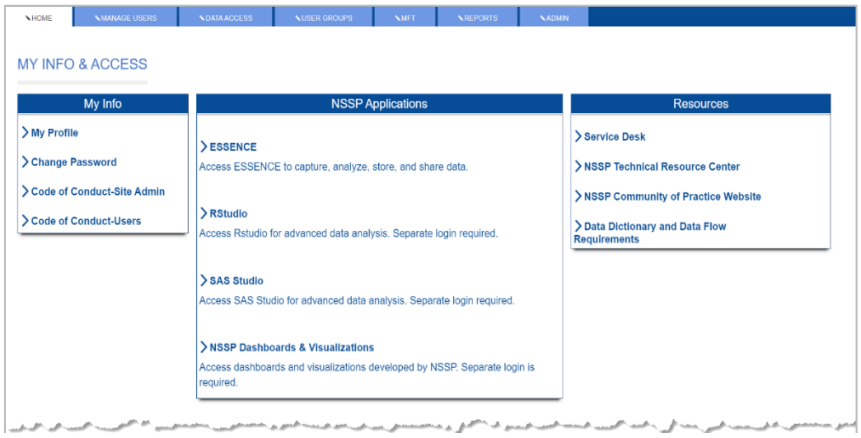


Figure 6. Site Administrator's Home Tab

3.3 Data You Can View in ESSENCE

Both the user and site administrator have a section at the bottom of their home page that allows them to see which data they can access via ESSENCE (Figure 7).

Rule Name	Rule Site	User Name	User Site	Data Source	Data Details	"WHERE" Statement (if applicable)
NSSP National View Aggregate Only		User01 (1st Last Name)	Your Site	Region Syndrome Alert List	N	
NSSP National View Aggregate Only		User01 (1st Last Name)	Your Site	Data Quality (HHS Region)	N	
NSSP National View Chief Complaint Query Validation		User01 (1st Last Name)	Your Site	Chief Complaint Query Validation	Y	
NSSP National View Mortality Keyword Syndrome Development		User01 (1st Last Name)	Your Site	Mortality Data (Keyword Syndrome Development)	Y	

Figure 7. Data You Can View in ESSENCE

4. Navigation

The AMC Home page is organized with tabs across the top. A list and description of each tab follows. Users only have access to the Home Tab, which is displayed after logging in, whereas site administrators and others with elevated privileges have access to additional tabs. Table 1 shows tabs available to each user type:

Table 1. Access to Tabs by User Privilege Level

User Type	Home	Manage Users	Data Access	User Groups	MFT	MFT Review	Reports	Admin (Full)	Admin (Usage)
User	✓								
MFT View Only	✓				✓ (View)				
MFT View/Edit	✓				✓ (View/Edit)				
Administrator	✓	✓	✓	✓	✓		✓		✓
Super Admin	✓	✓	✓	✓	✓	✓	✓	✓	✓

The Admin (Full) Tab has a drop-down sub-menu to select Notifications, Software Requests, and Software Usage. The Admin (Usage) Tab only has access to the Software Usage sub-menu.

4.1 Home Tab

The Home tab allows users and site administrators to do the following:

- View My Info,
- Navigate to NSSP Applications,
- Navigate to Resources, and
- View the user's data access rules for ESSENCE (data table at bottom of the Home Tab).

My Info

You may update your profile (certain fields only), change your password, and, for administrators, view both the Code of Conduct (CoC) for Site Administrators and the CoC for Users in PDF file format. (Users may only view the CoC for Users.)

NSSP Applications

Users and site administrators can gain quick access to tools and applications (ESSENCE, Posit [RStudio] Workbench, SAS Studio) and to NSSP dashboards and visualizations.

Resources

This section links to resources available to all users:

- Service Desk to request technical and general support
- NSSP Technical Resource Center for NSSP-specific onboarding materials, quick start guides, user manuals, and guidance documents
- NSSP Community of Practice Website for accessing the Knowledge Repository and for connecting with thought leaders and experts in analytics, informatics, and surveillance
- Data Dictionary and Data Flow Requirements

Data You Can View in ESSENCE

At the bottom of the Home page, there is a data table that enumerates the Data Access Rules that directly affect your access to the data in ESSENCE. All user types (user, site administrator, superuser [also known as operational access user], and MFT access user) are provided this information.

This table has the following columns:

- Rule Name—Names of specific data access rules that you or a user group that you are in have been assigned to.
- Rule Site—Except for rules created for the NSSP National View, the Rule Site is the site where the rule was created. Most often this will be your own site, but the Rule Site might differ if another site shares some of its data with you.
- User Name—This will show your AMC User ID and the name in your User Profile (in parentheses).
- User Site—This contains your site name.
- Data Source—The entries in this column correspond to one of the nine Data Sources that can be selected when creating a data access rule.
- Data Details—There is a Y for Yes or an N for No depending whether the data access rule assigning you access was set up to provide access to data details.
- "WHERE" Statement (if applicable)—If the data access rule is further constrained by use of one or more WHERE Clauses, those clauses will be listed here.

4.2 Manage Users Tab (Site Administrators Only)

The Manage Users tab (Figure 8) is available only to site administrators and superusers. This tab allows site administrators to create new accounts or to view, modify, or delete user accounts within their site. The site administrator can also download a Comma Separated Values (CSV) file for a list of users in their site.

Superusers may view, modify, or delete user accounts in any site and can generate a report listing users in all BioSense Platform sites or select a specific site to produce a more focused report.

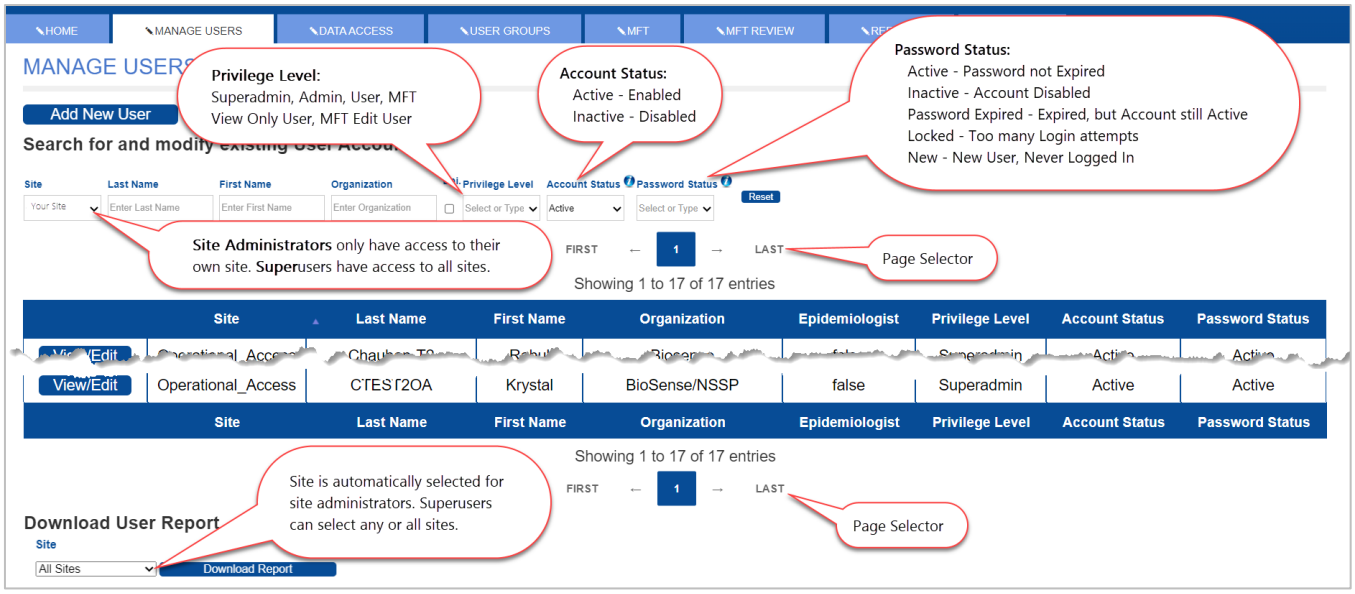


Figure 8. Manage Users Page

Create Users

To create a new user account, click **Add New User**, provide the requested information, and then click **Save**. Once you successfully save a new user, separate emails containing their new user ID and a temporary password will be sent to that user.

Things to remember when creating a new user:

- First Name, Last Name, and Email Address are required,
- You can only add users to your site,
- Each user within your site must have a unique email address; this means that a user cannot have two (or more) accounts with the same email address.

Modify User Accounts

To review or modify a user account, select a row in the user table and click **View/Edit**. You will be able to see and update the user profile.

When the Manage Users tab is first selected, a background routine selects all your site's users from the AMC database. Depending on the number of users in your site, this can take from several seconds to a minute or more to retrieve and display them in table form. When retrieval is complete, the search fields described below will no longer be greyed out. Please be patient.

Directly above the table of users, you will find search fields that can be used to dynamically filter your user base. To locate the user(s) you are interested in, you may use some or all the filter fields. Since the filters are dynamic, you may notice a short delay when you first start entering your filter criteria because the filtering process begins when you start typing.

4.2.1 Removing (Deactivating) User Accounts

Due to CDC policy, user accounts cannot be deleted. If a user no longer requires access, select the account by clicking the **View/Edit** button on the user's row, and change the **Account Status** radio button to "Inactive." **Note:** You must click **Submit** (at the bottom of the User Profile page) to complete the deactivation process. After you deactivate a user in the AMC, that user will no longer be able to use the AMC or other BioSense Platform tools.

4.2.2 User Profile Page

The User Profile page (Figure 9) displays a user's contact information and sections for account information and details.

4.2.2.1 User Profile

This section contains contact information and background. Those fields with a **red** asterisk (First Name, Last Name, Email Address, Organization, Site, Privilege Level, Foreign National, and Contractor) are required.

- *User Name*—The User Name required when logging into all BioSense Platform applications. The User Name is automatically generated by AMC and cannot be changed once a user's account has been created.
- **First Name*—The user's first name. This field is editable by the user and site administrators.
- **Last Name*—The user's last name. This field is editable by the user and site administrators.
- **Email Address*—The user's email address. Password expiration emails will be sent to this email address. This field is editable by the user and site administrators and must be unique within the site. Federal users are required to use their government email address.
- *Office Phone*—The user's contact phone number. This field is editable by the user and site administrators.
- **Organization*—The user's organization affiliation. This field is editable by the user and site administrators.

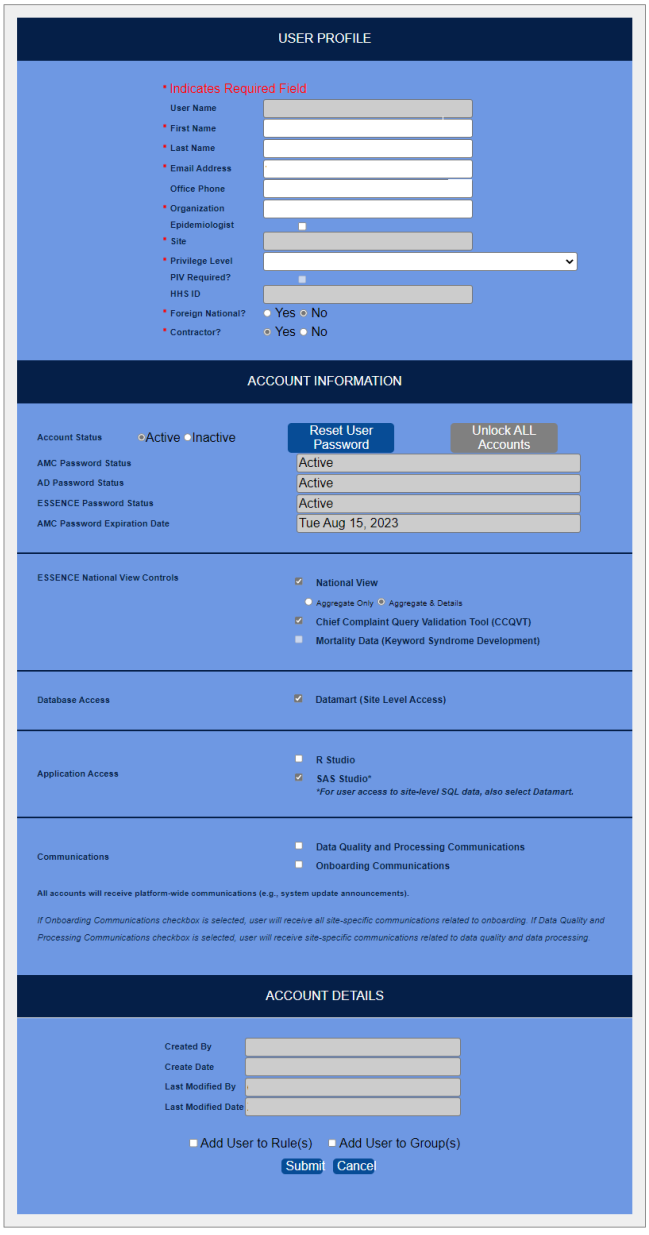


Figure 9. User Profile Page

- *Epidemiologist*—Box should be checked if the user is an epidemiologist. This will add the user to the site's epidemiologist data access rule. This field is editable by site administrators but NOT by individual users.
- **Site*—The site affiliation assigned to a user during account creation. If a user requires multiple site affiliations, multiple user accounts must be created. A user's site affiliation cannot be changed once a user's account has been created. Site administrators should contact the NSSP Service Desk if a change of site affiliation is required.
- **Privilege Level*—The level of access a user is granted for the BioSense Platform tools and applications. This field is only editable by NSSP staff. Site administrators may contact the NSSP Service Desk if a change of privilege level is required.
- *Primary Site Admin*—This checkbox is only presented to NSSP staff. When a site has multiple site administrators, this checkbox is used to designate one as the primary.
- *PIV Required?*—This checkbox is only editable by NSSP staff and would be selected if the user has a PIV card and is required to use a PIN code for logging in to both AMC and ESSENCE. Once checked, a field to enter the U.S. Department of Health and Human Services (HHS) ID become visible, and this number must be supplied.
- *HHS ID*—The user's HHS ID found on the back of the PIV card. This number is required if the "PIV Required" checkbox is selected. **Note:** This field is primarily used by CDC and other staff.
- **Foreign National*—"Yes" indicates that the user is a foreign national, whereas "No" indicates that the user is not. This is required for security purposes but does not alter permissions. This field is editable by site administrators but NOT by individual users. (A Foreign National is *anyone who is not a U.S. citizen, U.S. national, or immigrant who has been granted the right to permanently reside and work in the United States.*)
- **Contractor*—"Yes" indicates that the user is a contractor. "No" indicates that the user is not a contractor. This information is required for security purposes but does not alter permissions. The field is editable by site administrators but NOT by individual users.

4.2.2.2 Account Information

This section of the user's profile details information about the account and password status. To implement the BioSense Platform's single sign-on functionality, the AMC synchronizes passwords across the Active Directory, AMC, and ESSENCE. If any of the three password statuses show "Password Locked," a site administrator can click the **Unlock ALL Accounts** button to unlock accounts and change the password status to "Active." If any password statuses show "Password Expired," or if the user has forgotten the password, the site administrator can click **Reset User Password** to email the user a password reset link and temporary password.

- *Account Status*—When "Active," indicates the user's account is enabled. When "Inactive," the user's account is disabled. A site administrator can activate or inactivate a user's account by selecting the corresponding radio button and saving the profile. Only one can be selected. When a user's account status is "Inactive," he or she will be unable to log in to any of the applications on the BioSense Platform.
- ***Reset User Password** button*—Clicking this button will invalidate the current password, generate an email to the user with a temporary password, and force the user to choose a new password when next logging in.
- ***Unlock ALL Accounts***—If the user has accidentally locked the AMC account, it will be set to "Inactive." The site administrator can unlock it by clicking this button. This button will unlock the AMC account as well as all associated accounts, for example, ESSENCE, Posit (RStudio), and SAS Studio.
  This button is currently inactive.
- *AMC Password Status*—The status of the user's AMC account password (Password Status values: Active, Inactive, Password Expired, Locked, or New).
- *Active Directory Password Status*—The status of the user's Active Directory (AD) account password (AD Password Status values: Active, Inactive, Password Expired, Locked, or New).

- *ESSENCE Password Status*—The status of the user's ESSENCE account password (ESSENCE Password Status values: Active, Inactive, Password Expired, Locked, or New).
- *AMC Password Expiration Date*—The expiration date of the user's current password.

4.2.2.3 ESSENCE National View Controls

Site administrators may control which users can view the National View and Chief Complaint Query Validation data sources within ESSENCE. In addition, users may be given access to Mortality data here. **By default, users do not have access to these data sources.**

- *National View*—Select this option to allow the user to view the ESSENCE data sources "Patient Location (Limited Details by HHS Region)" and "Facility Location (Limited Details by HHS Region)." When this box is checked, you may select either the Aggregate Only or Aggregate & Details radio button:
  - *Aggregate Only*—Select this option to view the ESSENCE data sources "Patient Location (Limited Details by HHS Region)" and "Facility Location (Limited Details by HHS Region)" at an aggregate level (i.e., the user may view charts, graphs, and maps with no access to line-level data).
  - *Aggregate & Details*—Select this option to view the full details for the ESSENCE data sources "Patient Location (Limited Details by HHS Region)" and "Facility Location (Limited Details by HHS Region)" (i.e., the user may view charts, graphs, and maps as well as the line-level data).
- *Chief Complaint Query Validation Tool*—Select this option to allow the user to use this ESSENCE tool to view the "Chief Complaint Query Validation."
- *Mortality Data (Keyword Syndrome Development)*—Select this option to allow the user to view ESSENCE Mortality Data. If a site is not reporting Mortality Data, this checkbox will not be active.

The National View data sources contain limited fields that are aggregated to the HHS Region level. The intent is to provide a high-level national picture of syndromic surveillance data. Every site that sends data to the BioSense Platform is contributing to the National View data source.

The Chief Complaint Query Validation data source contains Chief Complaint and Discharge Diagnosis text to allow users to refine queries. No identifying information—such as age, region, facility, or sex—is available in this data source. Sites may choose NOT to include their data in the Chief Complaint Query Validation data.

The Mortality Data (Keyword Syndrome Development) contains mortality keyword syndromes to allow users to refine ESSENCE queries. No identifying information—such as age, region, facility, or sex—is available in this data source. Sites may choose NOT to include their data in Mortality Data.

4.2.2.4 Database Access

Site administrators may control which user accounts can access their site's data within the DataMart. **By default, user accounts do not have access to this data source.**

- *DataMart (Site-level Access)*—Select this option to allow users to access and run queries against their site's Datamart (MS SQL) tables. Users may access SQL tables by using built-in functionality in Posit (RStudio) Workbench. SAS Studio requires explicit site-level access. The checkbox for either Posit (RStudio) Workbench or SAS Studio should be checked if the user needs site-level access to these Datamart tables. Both may be selected.

- These options do not grant access to any custom SQL views for counties, facilities, or other data subsets developed by request. To grant user access to custom SQL views, site administrators must submit a Service Desk request.

4.2.2.5 Application Access

Site administrators manage which accounts have access to the Posit (RStudio) and SAS Studio applications. **By default, new user accounts do not have access to these tools.**

- *Posit (RStudio)*—When access is selected in the user profile and the change is submitted, a note (in green font) will be displayed next to Posit or RStudio saying "**Access Request Pending**." The NSSP support team manually assigns access. Further instructions are shown in the following text box.
- *SAS Studio*—Select this option then submit the change to request access SAS Studio. SAS Studio is used to visualize site-level SQL data. When SAS Studio is requested, the NSSP support team will manually set up access.
- **To provide a user with access to site-level SQL data for use by either Posit (RStudio) or SAS Studio, the site administrator should also grant access to the DataMart by checking the Datamart (Site-Level Access) checkbox in the user's User Profile.**

Access to the BioSense Platform's Posit Workbench and SAS Studio

When the site administrator checks either Posit (RStudio) or SAS Studio in the User Profile and presses **Submit**, the NSSP support team is notified. Only site administrators may request licenses for users by checking the Posit (RStudio) and SAS Studio checkboxes on the User Profile page.

If spare licenses are available, one will be assigned to this user and the NSSP support team will set up user access. Posit (RStudio) licenses are limited and assigned on a first-come, first-served basis.

Site administrators must grant access to the DataMart (see Section 4.2.2.4) whenever users request SAS Studio application. Although Posit (RStudio) can access these data with built-in functionality and direct API calls, we suggest you grant access to Datamart when access to either of these applications is granted.

4.2.2.6 Site-specific Communications

Site administrators may manage which user accounts receive site-specific communications. There are two categories in the Communications section:

A. *Data Quality and Processing Communications*—Select this option to allow a user to receive site-specific communications related to data quality and data processing, including:
   a. Daily BioSense Platform Site Processing Summary.
   b. Quarterly Executive Data Quality Summary.
   c. Monthly Data Quality Report emails (completeness, timeliness, validity).
   d. Miscellaneous data quality issue information.

B. *Onboarding Communications*—Select this option to allow a user to receive site-specific communications related to onboarding, including information about

a. Data validation and facility management emails (that is, day-to-day onboarding operations).
b. Connectivity and technical assistance emails (for example, feed setup).
c. Strategic onboarding initiatives emails (for example, baseline cleanups).

Note: NSSP sends system updates and announcements to *all* account users.

4.2.2.7 Account Details

The Account Details section of the user profile provides information about creation and subsequent modification of the user account.

- *Created By*—The site administrator who created the displayed user account.
- *Create Date*—The date the user account was created.
- *Last Modified By*—The last user to have modified the displayed user account. This could be a site administrator or the user.
- *Last Modified Date*—The date the user account was last modified.

4.2.3 Add User to Rule(s) or Group(s)

Functionality has been introduced to facilitate adding a user to multiple existing Data Access Rules or User Groups while creating or editing a user's profile. At the bottom of the User Profile page (just above the Submit and Cancel buttons), you will note two checkboxes:

- Add User to Rule(s)
- Add User to Group(s)

You may toggle between these options, but only one of these checkboxes can be selected at a time. When you choose one, you will be taken to a page that will offer the option of adding multiple rules or user groups to the user's profile.

4.2.3.1 Add User to Rule(s)

If the Add User to Rule(s) box is checked and the Submit button is pressed, the DATA ACCESS tab opens and the message "ADD USER TO RULES," followed by "Successfully added (or updated) user '*UserName*' " is displayed.

Figure 10 shows a sample of the "ADD USER TO RULES" table before rule choices are selected. You must check each individual Data Access Rule you wish to add this user to, then click the **Submit** button.

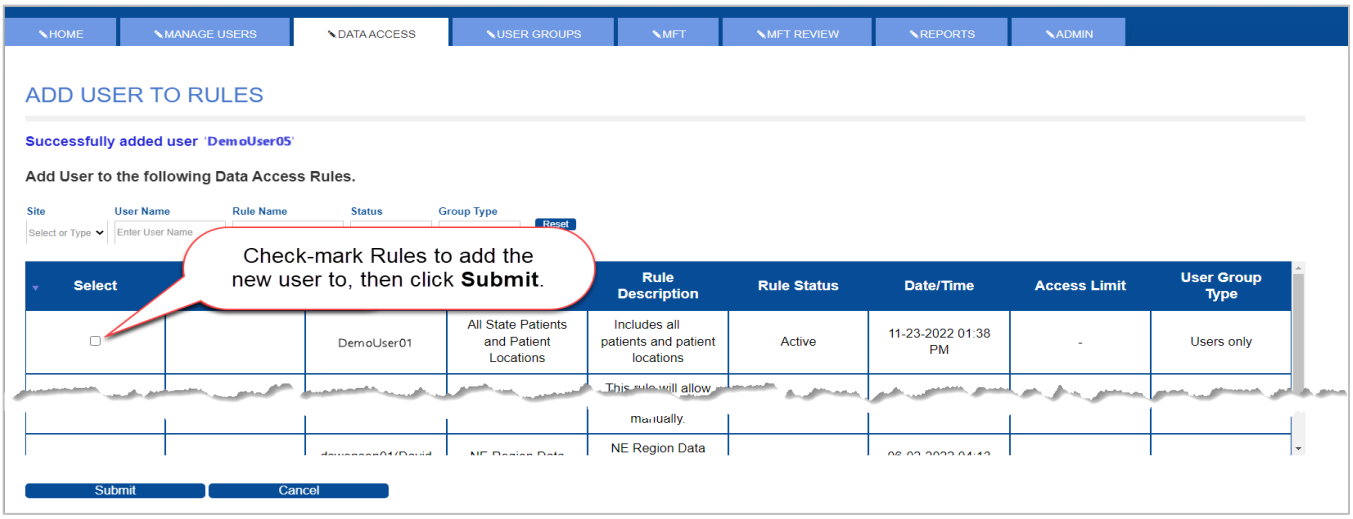


Figure 10. Add new user to Rules on Selection Page, then click **Submit**.

In the example for DemoUser05 (Figure 10), after the site admin clicks submit, the message "Successfully added (or updated) user 'DemoUser05'" will change to "User 'DemoUser05' has been added to the rule(s):" and the added rules will be listed. The selected rules remain checked in the table but are greyed out.

> **Note**: If the *Add User to Group(s)* checkbox on the User Profile is already checked, it will be unchecked when you check the *Add User to Rule(s)* checkbox. In other words, you may toggle between these two options but cannot select both.

4.2.3.2 Add User to Group(s)

When this box is checked and the **Submit** button is pressed, the USER GROUPS tab opens to display the following message: "ADD USER TO GROUP(S)," followed by "Successfully added (or updated) user '*UserName*'." You must mark each individual group in the *My Site User Groups* table that you wish to add this user to, then click **Submit**.

The message under "ADD USER TO GROUP(S)" will change to "User *'Username' has been added to the group(s):"* and the group(s) you checked will be listed in the table underneath (Figure 11). In addition, the group(s) you added this user will be greyed out in the table of User Groups.

Note: AMC keeps track of which user groups each user is assigned to. If you use this functionality to add a user to a group that they already belong to, the "ADD USER TO GROUP(S)" page will display those groups, but they will be grayed out. That is, you cannot add them to the same group twice.

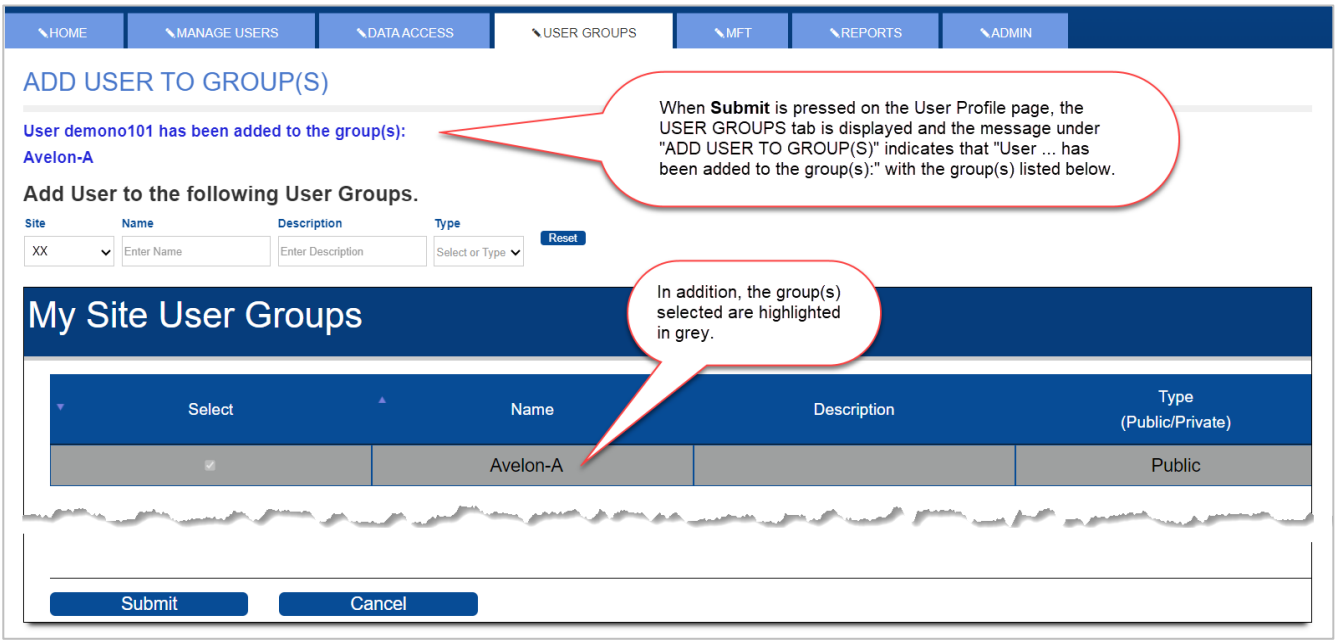


Figure 11. User Successfully Added to One Group in My Site User Groups

4.2.4 User Report

At the bottom left of the Manage Users page, you will note the Download User Report section (Figure 12) with a drop-down to select a site. As a site administrator, you only have access to your site. To generate a report of all your users, click the **Generate Report** button. When you click on the button, a CSV file will automatically be generated and downloaded to your default download folder. This file can be viewed using a text editor, Excel, or another spreadsheet program. Note that the download file created is named:

User_<your AMC user name>_<your site's short_name>_yyyy-mm-dd

For example, *User_adandy01_XX_2023-03-15.csv*

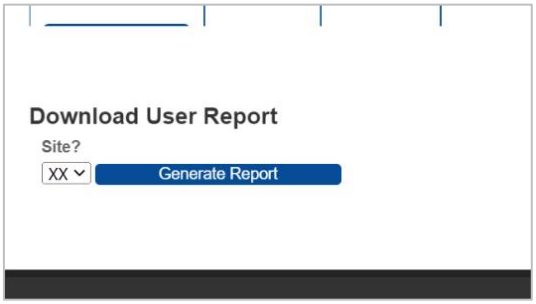


Figure 12. Generate and Download User Report

Table 2 (read from left to right) lists the fields exported to the CSV file.

Table 2. Fields Exported to User Report

Login	PIV_Required	First_Name	Last_Name	Organization	Email
Telephone	Last_Login _Date	Conduct_ Accepted_Date	Account_ Active_Text	Password_ Status_Text	Privilege_ Name
Site_ID	Site_ Short_Name	Site_Name	Epidemiologist	National_ View_Aggregate	National_ View_Detail
Chief_Complaint_ Query_Validation	Mortality_KSD	RStudio*/ Posit	Primary_ Site_Admin	Creator	Contractor
Foreign_National	DQProcessing_ Communications	Onboarding_ Communications	Last_Edited_By	Date_Added	Date _Updated

** RStudio is rebranding to Posit.*

4.3 Data Access

The Data Access tab provides functionality to create new data access rules and to view, delete, or edit existing rules. These rules are used to provide your users and user groups with access to your site's data. In addition, rules can be set up to provide limited access to users and user groups from other sites within the BioSense Platform.

The Data Access tab is only available to site administrators and operational access users (superusers). As a site administrator, you may use this tab to create, review, edit, and delete rules that control access to your site's data (Figure 13). Note the **red** arrows pointing to the **Build New Data Access Rule** and **View/Edit** buttons.

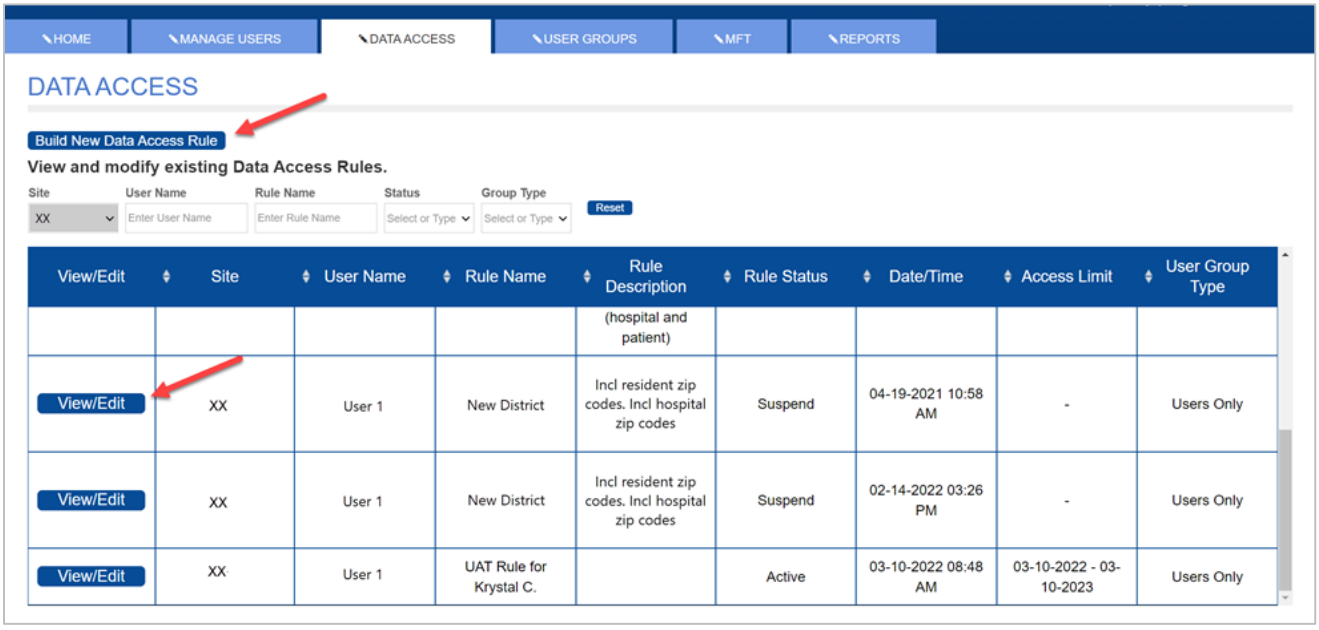


Figure 13. Build New Rule or View/Edit an Existing Rule

Typically, site administrators set up a general data access rule for all the site's regular users. Then the site administrator can add user IDs or user groups to this general user data access rule. Later, other rules may be needed to provide additional specific access.

One of the site administrator's tasks, when a new user is added, is to add the new user to the general access rule. Or, if a new user's data access requirements differ from the regular users and the available access rules, the site administrator can create new rules for them. This task is necessary when adding new users to your site. If existing rules will provide needed access, this can now be handled with functionality available at the bottom of the User Profile page (see Section 4.2.3 for details).

Dynamic filtering is available for Site, User Name, Rule Name, Status, and Group Type. You may notice a small delay as you start typing filter criteria, since the filtering process begins when the first character is entered in a search field.

The User Name column was added to identify the rule creator or the name of the last person to edit the rule. The *Date/Time* column shows the date the rule was created or last modified.

4.3.1 Create a Data Access Rule

If an existing data access rule does not provide the exact access needed, a new data access rule can be created to provide this access for a specific user, or user group, or when providing access to your site's data for users in other sites.

The preferred method for sharing data across sites (or with different public health jurisdictions) via the BioSense Platform is to create a data access rule—or multiple rules—for the users from those sites that need access to your data. NSSP does not recommend creating a user ID within your site for a user in a different state or public health jurisdiction. This can create maintenance issues over time.

Data access rules can be applied to your site's users and to other user accounts across the BioSense Platform. In other words, you may create rules to grant data access to analysts and epidemiologists who work at your site, another site, or at CDC.

Note: The *Access Limit* field, displayed on the table of rules presented on the Data Access tab, is only populated for rules where a *Data Access Time Limitation* is specified.

4.3.1.1 Rule Name and Description

Name your rule and enter a description (Figure 14). A descriptive name and detailed description will help you find your rule later.

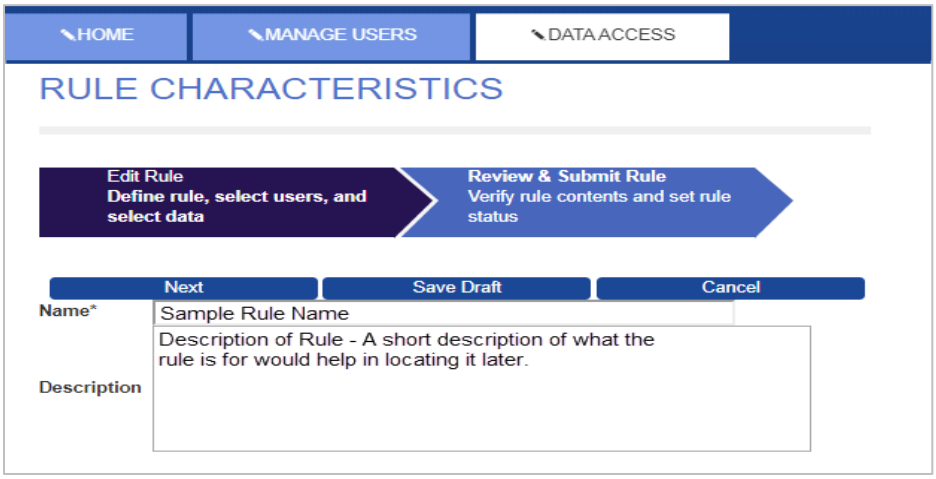


Figure 14. Name Your Rule and Add a Short Description

4.3.1.2 Data Access Time Limitation

This functionality allows the site administrator to give data access to a user or user group for a specified amount of time or between two dates.

For example, you may grant access to your site's data for a week, six months, or a year from the drop-down list (Figure 15), or you can enter a custom date range during which they will have access to the dataset defined by the data access rule.

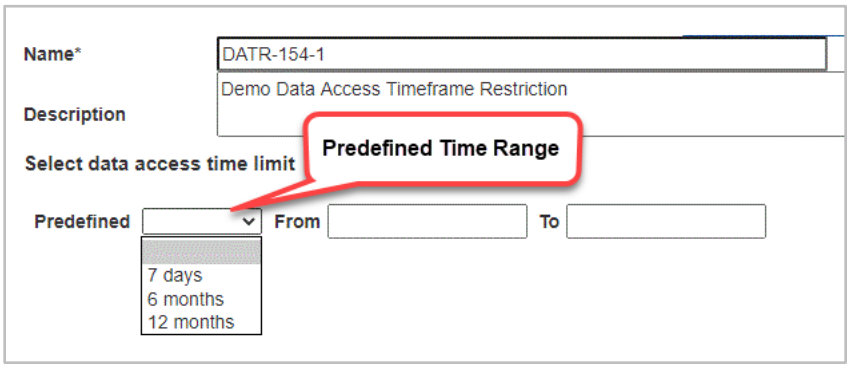


Figure 15. Predefined Time Range

To enter a custom data access period, manually enter the start (From:) and end (To:) dates in the fields as shown in Figure 16. Note that a pop-up calendar is displayed when you select each field, and you may select dates directly from the calendar.

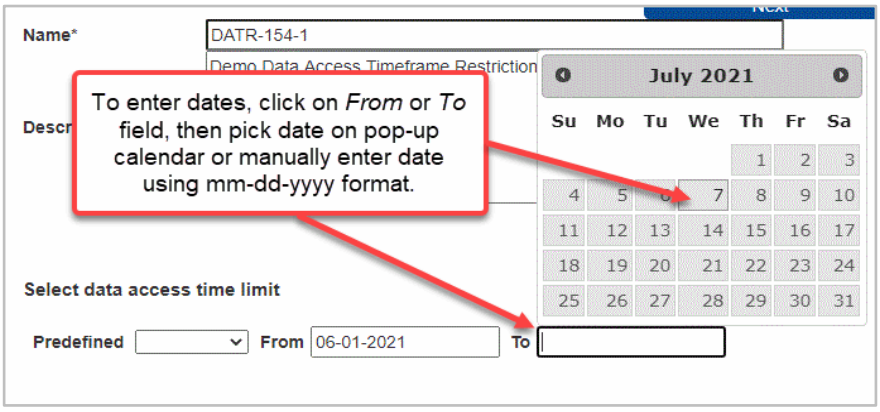


Figure 16. Date-specified Time Range

Note: When the current date falls outside the specified date range, the data access rule status will automatically be set to "Suspend."

4.3.1.3 Select Users and User Groups

When selecting Users or User Groups (explained below), click the large **blue** plus sign (**+**) to expand the Users or User Group sections (Figure 17). If desired, you may expand both Select Individual Users and Select a User Group at the same time.

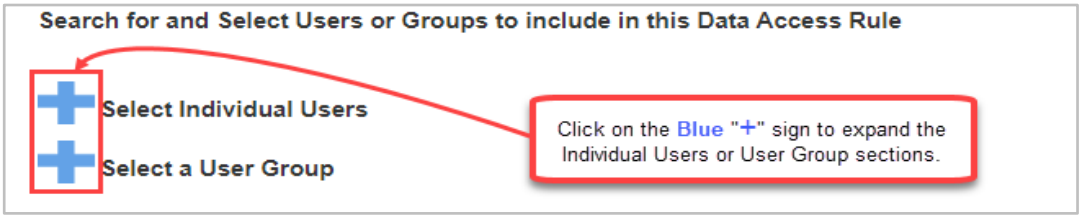


Figure 17. Expand Users or Groups

Data should be shared with *purpose.* Carefully consider who needs access to your data and whether they should be included in a data access rule. Keep in mind that any user or group selected here (Figure 17), whether a member of your site or not, will receive access to the data source(s) you specify in the next step for the rule you are creating.

Note: You can add users or user groups to an existing rule if its parameters will provide the specific data they require.

There can be site-defined user groups (*Public* or *Private*) and NSSP user groups to choose from. Users and user groups are listed by site. Both sites and the user names within a site are sorted alphabetically.

You may use the search fields directly below "Select Individual Users" and "Select a User Group" headings to filter the "Available" lists. These filters are dynamic, and the Available pick box selections narrow as each character is typed.

> Be aware when searching for the Last Name or First Name of a user, results can have the characters that you enter appearing in any contiguous location within the name (for example, "**an**" will find ***An***derson and Stedm***an***, but not M***a***dde***n***).

Click on your choice in the "Available" pick boxes (or use Ctrl-Click for multiple choices within a pick box). This will highlight each choice (Figure 18). **Note:** Site-defined user groups must be created prior to adding them to a data access rule.

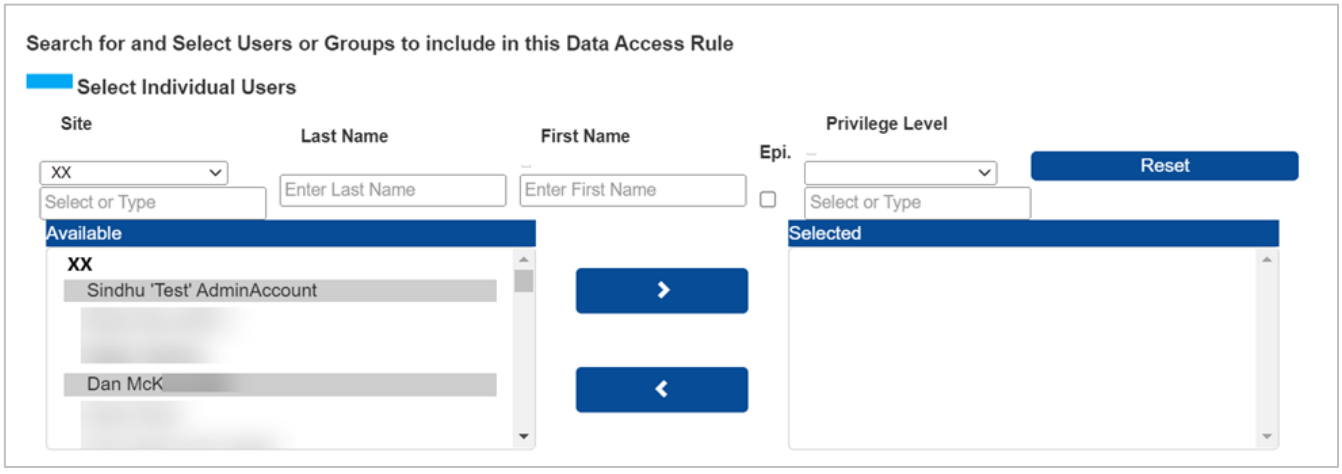


Figure 18. Data Access Page (Rule Characteristics—Select Users and Groups)

After highlighting users and groups in the “Available” box, click the “right” arrow button (**>**) shown between the pick boxes to move the highlighted names or groups to the “Selected” box (Figure 19). You may select more than one individual or group and move them (**>**) from the “Available” pick box to the “Selected” pick box. Similarly, to deselect them, you may move them back (**<**) from “Selected” to “Available.”

You may change the selected users or groups at any time.

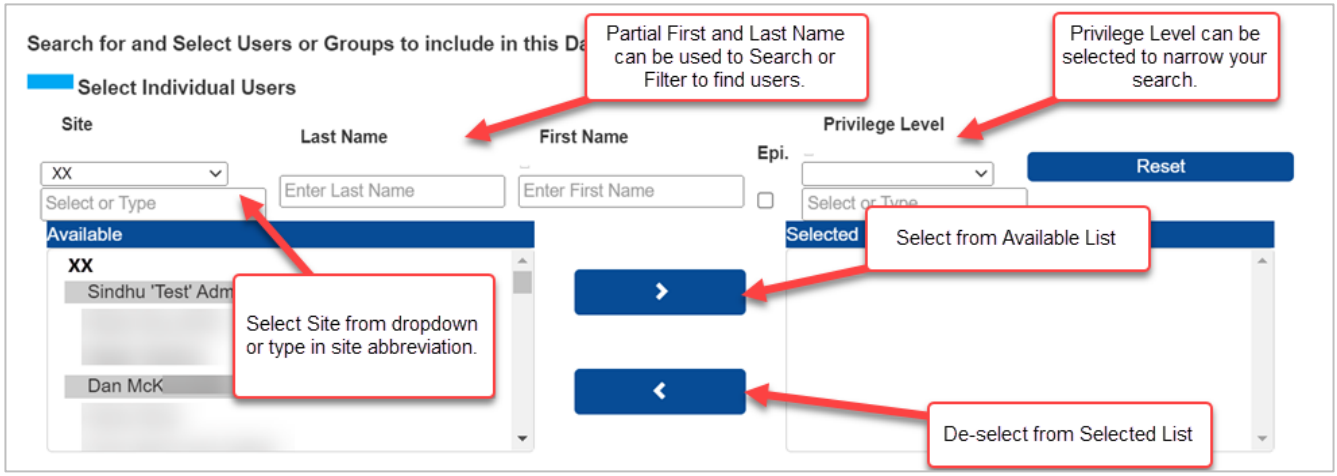


Figure 19. Selecting Users from "Available" Pick Box

4.3.1.4 Selecting Data Sources

Next, select the data source(s) you want included in the data access rule (Figure 20). Be mindful that you can only control access to your site’s data. You may grant users access to all your data sources or to individual data sources and can provide that access with Data details or No data details. You may also restrict users from general access to your site’s data by facility, state, county, timeframe, or other parameters, as necessary.

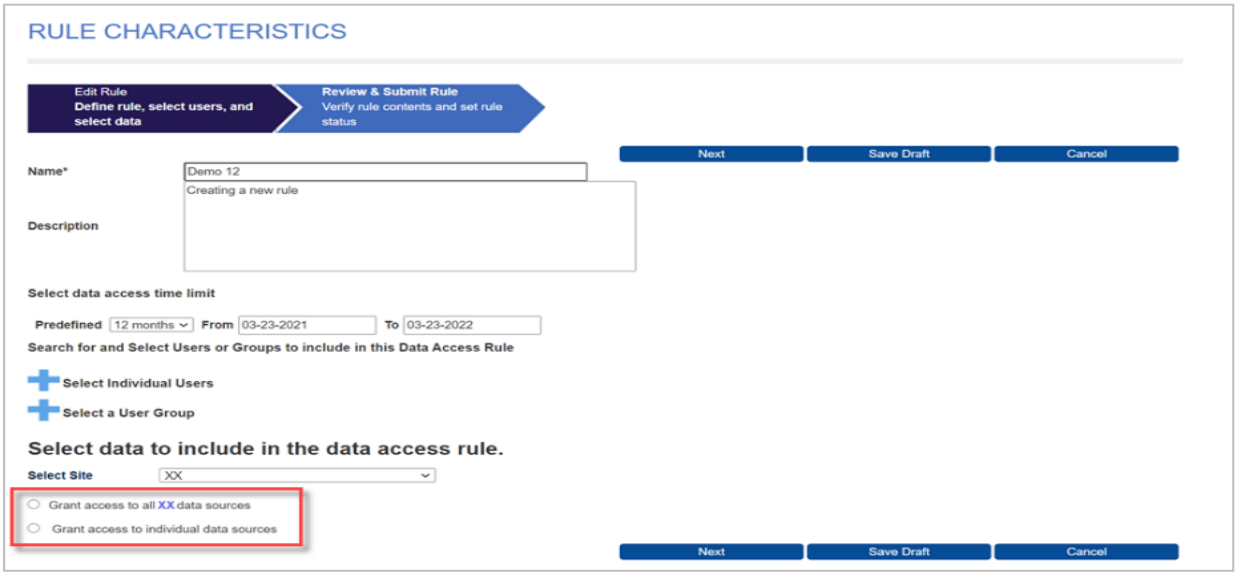


Figure 20. Data Access Page—Select Data

Note: The text box on the next page contains more information about Details, No data details, and data layers.

4.3.1.5 Access to All Data Sources

Site administrators have the option to grant access to all data sources (Figure 21) in a single step. Do this by clicking the **Grant access to all data sources** radio button. Once selected, you must choose the Data details, or the No data details data layer.

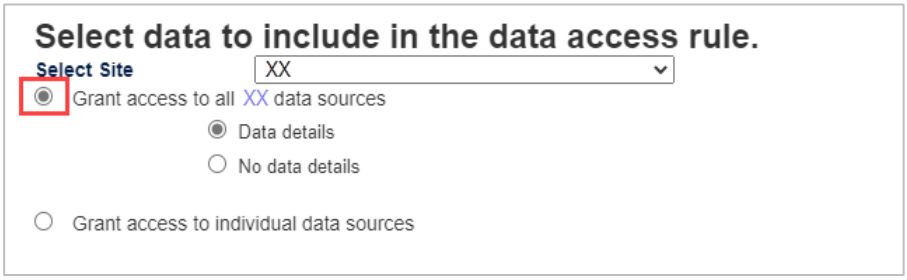


Figure 21. Data Access Page (Grant Access to All Data)

What is the difference between "Data details" and "No data details"?

"No data details" and "Data details" are called **data layers**. The "No data details" data layer provides a restricted view of the available data, whereas the "Data details" data layer provides access to the full set of data in ESSENCE. Of course, access to data can be further restricted by the use of WHERE clauses.

By selecting "No data details," affected users can only view high-level data in ESSENCE via charts, graphs, and maps. Users will NOT have access to line-level data. For example, when running a query against a data source where "No data details" was selected, users cannot click on graphs to view detailed data, such as patient information.

4.3.1.6 Access to Individual Data Sources

Site administrators have the option to grant access to an individual data source or to multiple data sources. To grant access to individual data sources, click the **Grant Access to Individual Data Sources** radio button and then click the checkboxes next to the desired data sources to grant access (Figure 22). When you click a checkbox, it will expand the data source. There you can select the data layer and apply optional data restrictions for each data source selected.

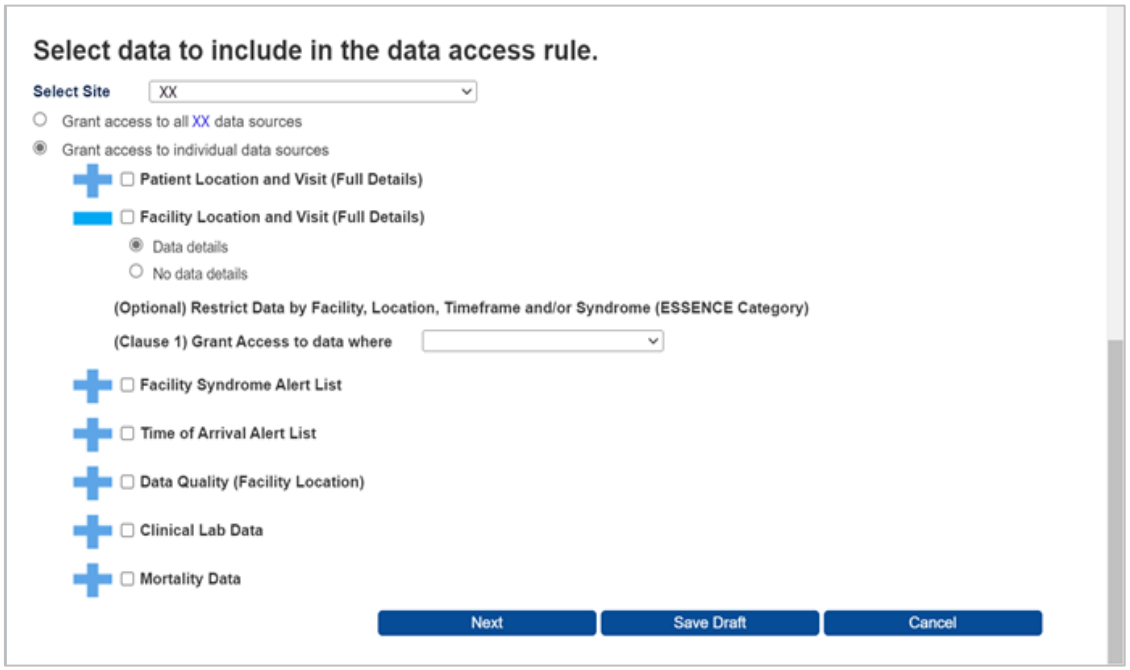


Figure 22. Data Access Page (Grant Access to Individual Data Sources)

Note: The text box on the following page describes the data sources currently available.

Data Source Definitions

- ***Patient Location and Visit (Full Details)***—Provides access to data based on where the patient lives. A user granted **Data details** access to this data source may view a complete list of patient details for all patients visiting your site's facilities. Restrictions made *after* selecting the dataset (for example, by facility, state, county, or syndrome) will be applied based on the location of the patient. If the **No data details** radio button is selected, a restricted view is provided.
- ***Facility Location and Visit (Full Details)***—Provides access to data based on the facility (for example, emergency department) location where a patient sought treatment. A user granted **Data details** access to this data source may view a complete list of patient details for all facilities located in the corresponding site. Restrictions made *after* selecting the dataset will be applied based on the location of the facility. If the **No data details** radio button is selected, a restricted view is provided.
- ***Facility Syndrome Alert List***—Provides access to public health event alerts by facility or syndrome for the corresponding site. A site administrator may control the alerts based on the location of the facility.
- ***Time of Arrival Alert List***—Provides access to public health event alerts by time of arrival for the corresponding site. A site administrator may control the alerts based on the facility location.
- ***Data Quality (Facility Location)***—Provides access to multiple data quality metrics, including completeness of data (by variable, by location, etc.), whether data are mapped to known values, and status of data processing by facility.

Note: Clinical Laboratory Data and Mortality Data are not available to the U.S. Department of Defense (DOD), U.S. Department of Veterans Affairs (VET), or Assistant Secretary for Preparedness and Response (ASPR) sites.

- ***Clinical Laboratory Data***—Provides access to laboratory orders and results for patients who live within a state (Patient State) and county (Patient County), as well as data collected from providers within the state (Provider State). Since all sites in multi-site states have access to the laboratory data collected by providers within that state, each site may grant access to all data for the state by creating a where clause using Provider State. Provider data cannot be limited below the state level.
- ***Mortality Data***—This data source provides access to mortality data from each state's Office of Vital Statistics or equivalent. It is organized by state and county. Any site within a state will be able to grant access to all mortality data recorded for deaths in that state.
- ***CELR***—This data source provides access to the COVID-19 Electronic Laboratory Reporting (CELR) data.

4.3.1.7 Data Access Timeframe Restriction

Access can be granted to data in your site for records from a certain timeframe based on the source of the data. Below (Table 3) is a list of sources and the dates used in ESSENCE to specify the records to be included within the timeframe.

Table 3. Data Check-In Dates in ESSENCE for Data Access Timeframe Restrictions by Data Source

Source of Data	Date Checked in ESSENCE (Date Type)
Patient Location and Visit	Date of Visit
Facility Location and Visit	Date of Visit
Clinical Laboratories	*Earlier date between* Lab Order Date and Results Date
Mortality	Death Date
Facility Syndrome Alert List	Date of Visit
Data Quality	Date of Visit
Time of Arrival Alert List	Date of Visit
COVID-19 Electronic Laboratory Records	*Earlier date between* Lab Order Date and Results Date

The *timeframe* can be open or closed. For example, you may manually enter the start date (Timeframe-From) without an end date to allow ESSENCE to select all records from the Timeframe-From date forward. Or you may enter only an end date (Timeframe-To) without a start date to constrain the selection to all records up to that date.

To select a closed timeframe option, enter two clauses, Timeframe-From and Timeframe-To dates. This is used to initiate a search for all records with a date within that range. That is, ESSENCE will only show records with dates within that timeframe. The dates will be selected using the date type noted in the table above.

Please note that, when entering both start and end dates, the end date should be the same as or later than the start date. If not, the dates will automatically be changed to be the same.

When entering dates manually, use this format: mm-dd-yyyy.

The data access timeframe restriction (Figure 23) can be chosen after you have selected a particular data source.

When you click into the From or To fields, a pop-up calendar is displayed.

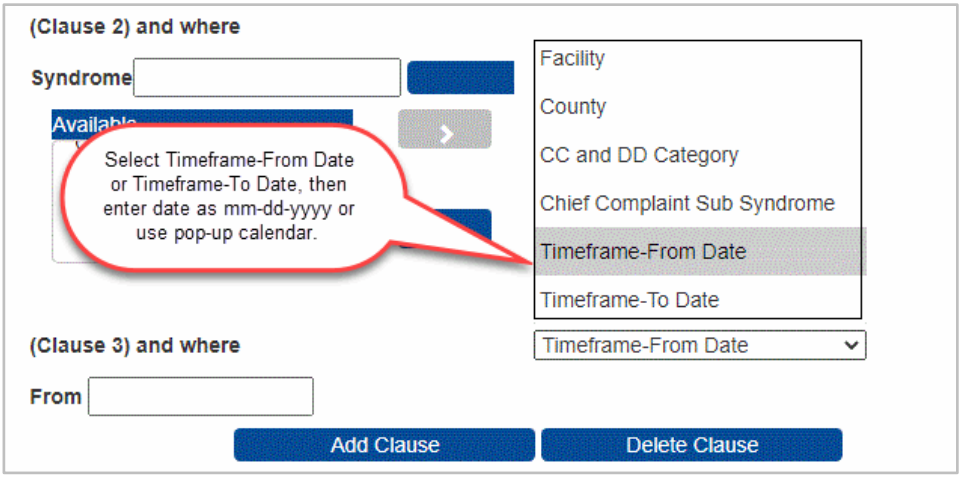


Figure 23. Setting up a Data Access Timeframe Restriction for a Data Source

4.3.1.8 Restrict Data by Facility or Location

Once the data source and data layer are selected, site administrators can optionally restrict the data source by Facility or Location (state and county) (Figure 24). To apply these optional restrictions, select Facility or Location (state and county). Then use the pick boxes to select the desired facilities or locations. Once the data source and data layer are restricted, click the **Add Clause** button. You can review your rule's data selection criteria on the "Review & Submit Rule" page (Section 4.3.2).

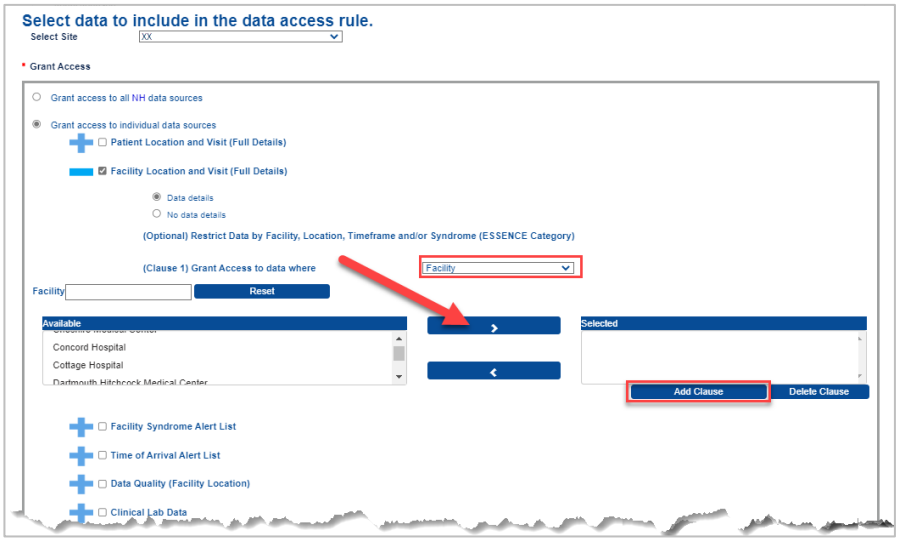


Figure 24. Data Access Page (Grant Access to Individual Data Sources)

Table 4. WHERE Clause Types Available in Data Sources

Data Source	Data Details	No Data Details
Patient Location and Visit (Full Details)	State, County, Facility, CC and DD Category, Syndrome, Chief Complaint Sub Category, Timeframe-From Date, and Timeframe-To Date	State, County, Facility, Timeframe-From Date, and Timeframe-To Date
Facility Location and Visit (Full Details)	State, County, Facility, CC and DD Category, Syndrome, Chief Complaint Sub Category, Timeframe-From Date, and Timeframe-To Date	State, County, Facility, Timeframe-From Date, and Timeframe-To Date
Facility Syndrome Alert List	State, County, Facility, Timeframe-From Date, and Timeframe-To Date	*Data/No Data Details not selectable*
Time of Arrival Alert List	State, County, Facility, Timeframe-From Date, and Timeframe-To Date	*Data/No Data Details not selectable*
Data Quality (Facility Location)	State, County, Facility, Timeframe-From Date, and Timeframe-To Date	*Data/No Data Details not selectable*
Clinical Laboratory Data	Patient County, Patient State, Provider State, Timeframe-From Date, and Timeframe-To Date	Patient County, Patient State, Provider State, Timeframe-From Date, and Timeframe-To Date
Mortality Data	State, County, Timeframe-From Date, and Timeframe-To Date	State, County, Timeframe-From Date, and Timeframe-To Date
COVID-19 Electronic Laboratory Reporting (CELR)	Timeframe-From Date, and Timeframe-To Date	Timeframe-From Date, and Timeframe-To Date

4.3.1.9 Access to Multiple Data Sources

To add additional data sources (Figure 25), click the checkbox next to the data source. This will expand the data source and let you select the data layer and apply optional data restrictions.

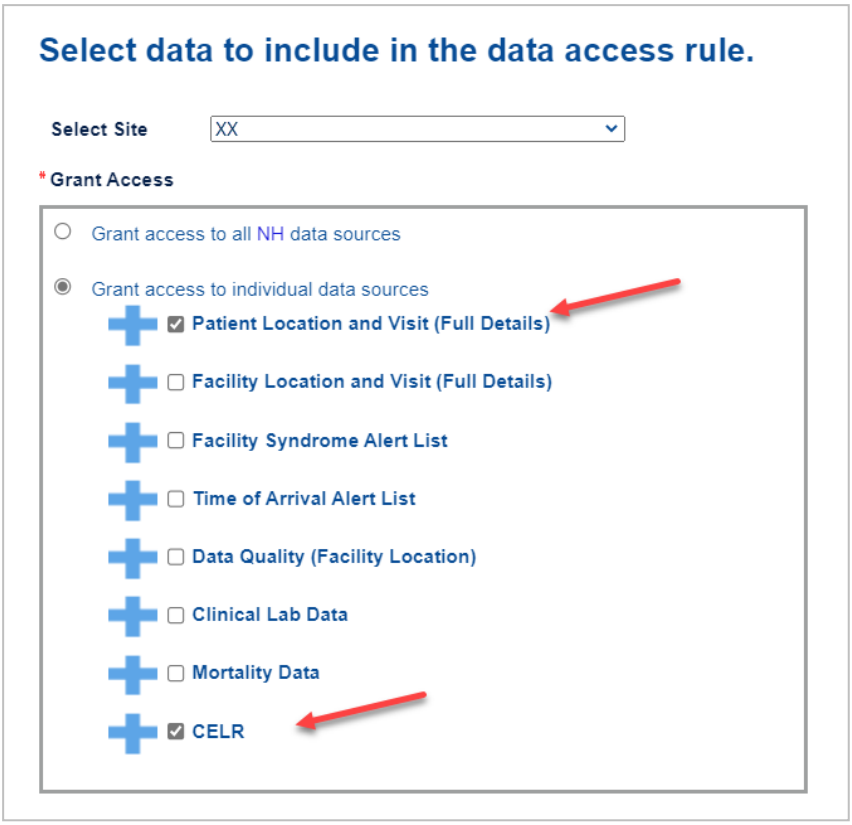


Figure 25. Data Access Page (Grant Access to Individual Data Sources)

After all selections have been made, click the **Next** button. **Note:** You may click the **Save Draft** button to save your work and return later.

4.3.1.10 Selecting Syndromic Restrictions

Syndromic restrictions can be applied to users or user groups by choosing "Grant access to individual data sources" and then selecting either Patient Location and Visit (Full Details) or Facility Location and Visit (Full Details). Next, choose the "Data details" data layer. Syndromic restrictions can then be applied by selecting "CC and DD Category," "Syndrome," and "Chief Complaint Sub Syndrome" for the WHERE clause.

Note: "CC and DD Category," "Syndrome," and "Chief Complaint Sub Syndrome" are only available if the "Data Details" data layer is selected.

Both "Data details" and "No data details" selections continue to provide other restrictions, such as State, County, Facility, and Timeframe restrictions.

As seen in Figure 26, when you choose **(1)** "Grant access to individual data sources" and select **(2)** "Data details," then **(3)** click the **Grant Access to data where** drop-down list, the additional syndromic selections are displayed:

- CC and DD Category
- Syndrome
- Chief Complaint Sub Syndrome

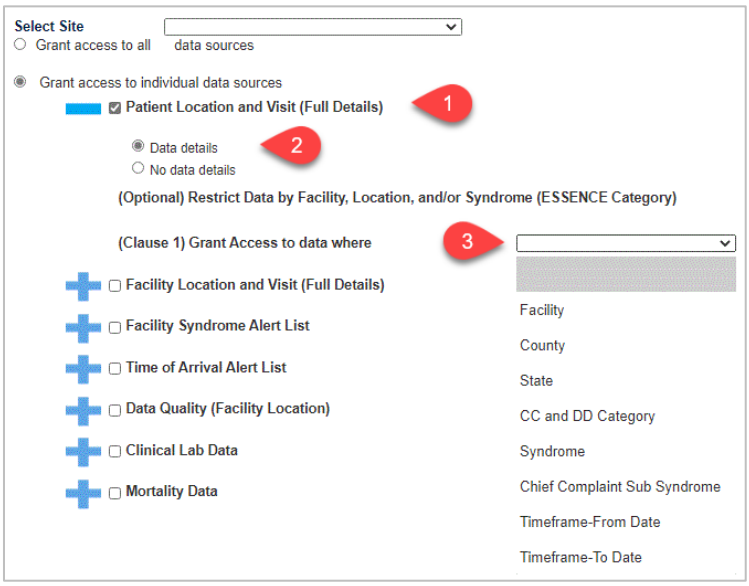


Figure 26. Data Access—Building the WHERE Clause

This allows up to eight (8) restricting clauses to be specified and, in addition to the syndromic selections, include Facility, County, State, and Timeframe–from Date and Timeframe–To Date.

Facility, County, and State values may include multiple selections. To do this, use Ctrl-Click or Shift-Click to highlight those values needed or add them sequentially by selecting each one individually and clicking the arrow (**>**) to add them.

When adding a CC and DD Category, Syndrome, or Chief Complaint Sub Syndrome, only one value may be chosen for each WHERE clause. Note that a warning message in **red** will be displayed at the bottom of the page stating, "**Only one selection is possible for this clause.**" (Figure 27).

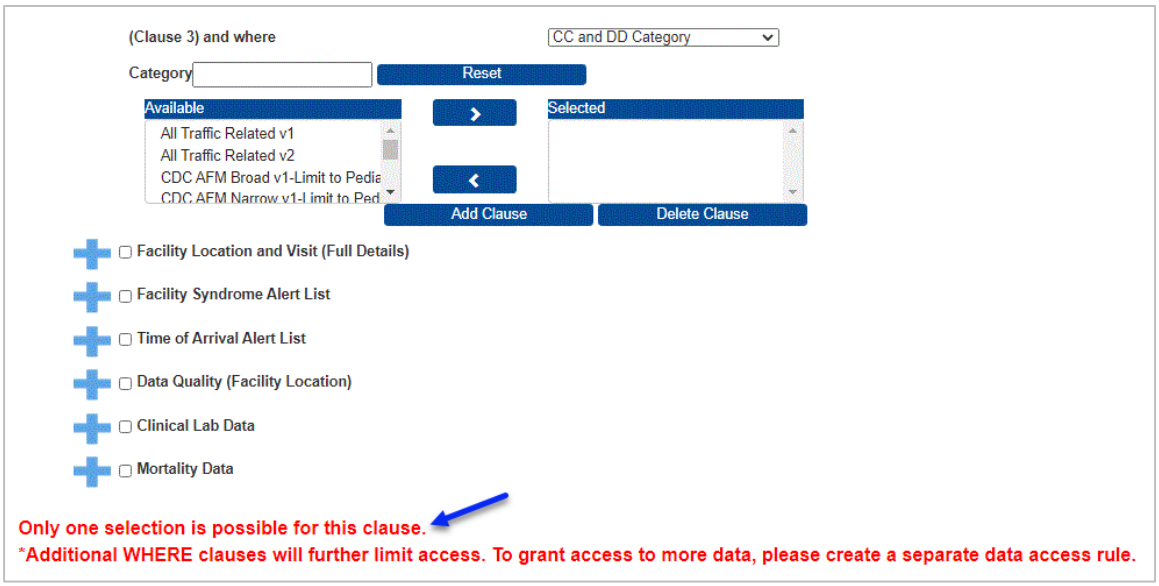


Figure 27. Data Access Rule—Only One Selection Message

4.3.1.11 Selecting Clinical Laboratory Data

Clinical lab data source data sharing capabilities have been added to the AMC. Users and site administrators may access clinical lab data for patients who live within a state (Patient State or County) and clinical lab data collected within the state (Provider State).

The following applies to site administrators and administrators with operational access (superusers). These administrators are now able to:

- Create data access rules in AMC for Clinical Laboratory Data that can include WHERE clauses for Patient State, Patient County, and Provider State shown in Figure 28.
- Edit an existing rule to:
  - Add states and counties to be included in a data access rule.
- Remove clauses (for example, if access is granted to data where Patient County = B, the site administrator or a super administrator can remove the clause that states "WHERE Patient County = B").
- Access ESSENCE and query the lab data specified in applicable data access rules including line-level data if access to Data details was granted.

Figure 28 provides an example of creating a new Clinical Laboratory Data rule.

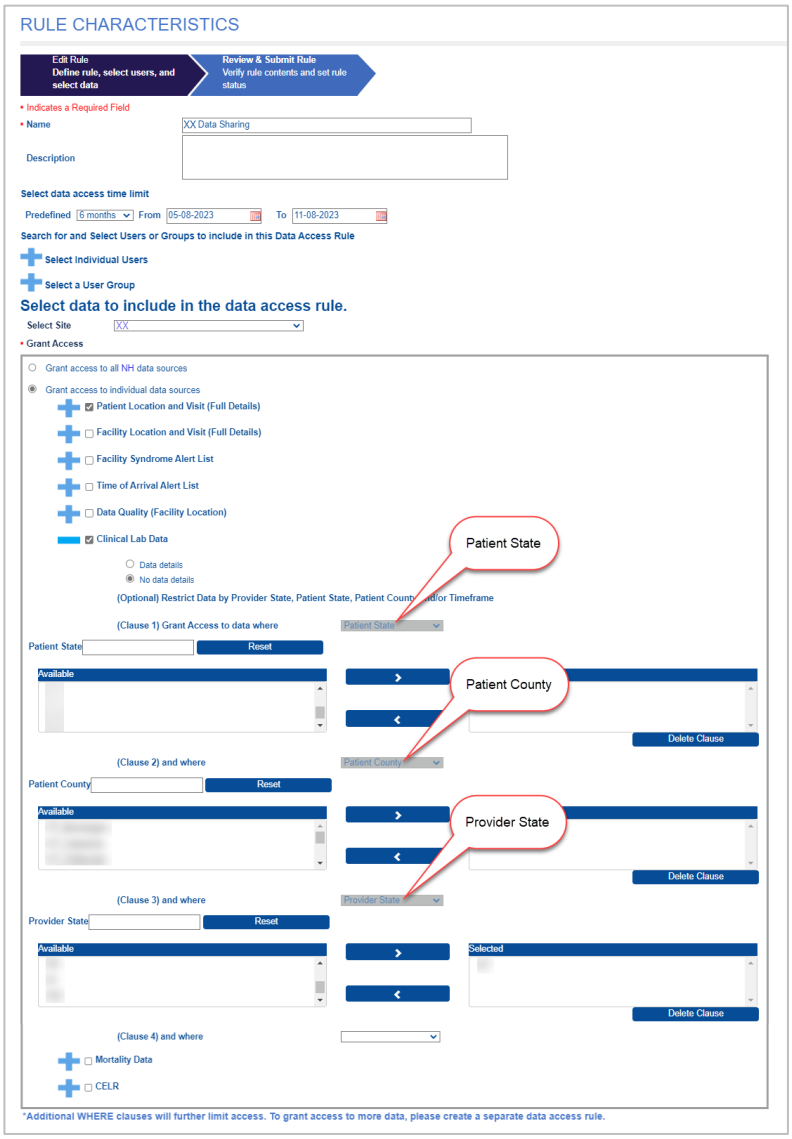


Figure 28. Data Access Build New Rule—Share Clinical Lab Data for Patients Residing in a Neighboring State

4.3.1.12 Selecting Mortality Data

The BioSense Platform receives electronic mortality data from several states. These data will enable more timely and robust analysis and response to public health events. Once received, mortality data can be integrated with illness, injury, and other health-related data, offering public health departments the opportunity for enhanced surveillance.

Where available, super administrators and site administrators can grant access to their state mortality data. Access is limited by state and county and can be further limited to specific timeframes. Figure 29 illustrates a clause used to provide access to select users.

When granted access, users may view mortality time series reports in ESSENCE. When provided access to data details, these same users may also view detailed information from the mortality records in the specified areas.

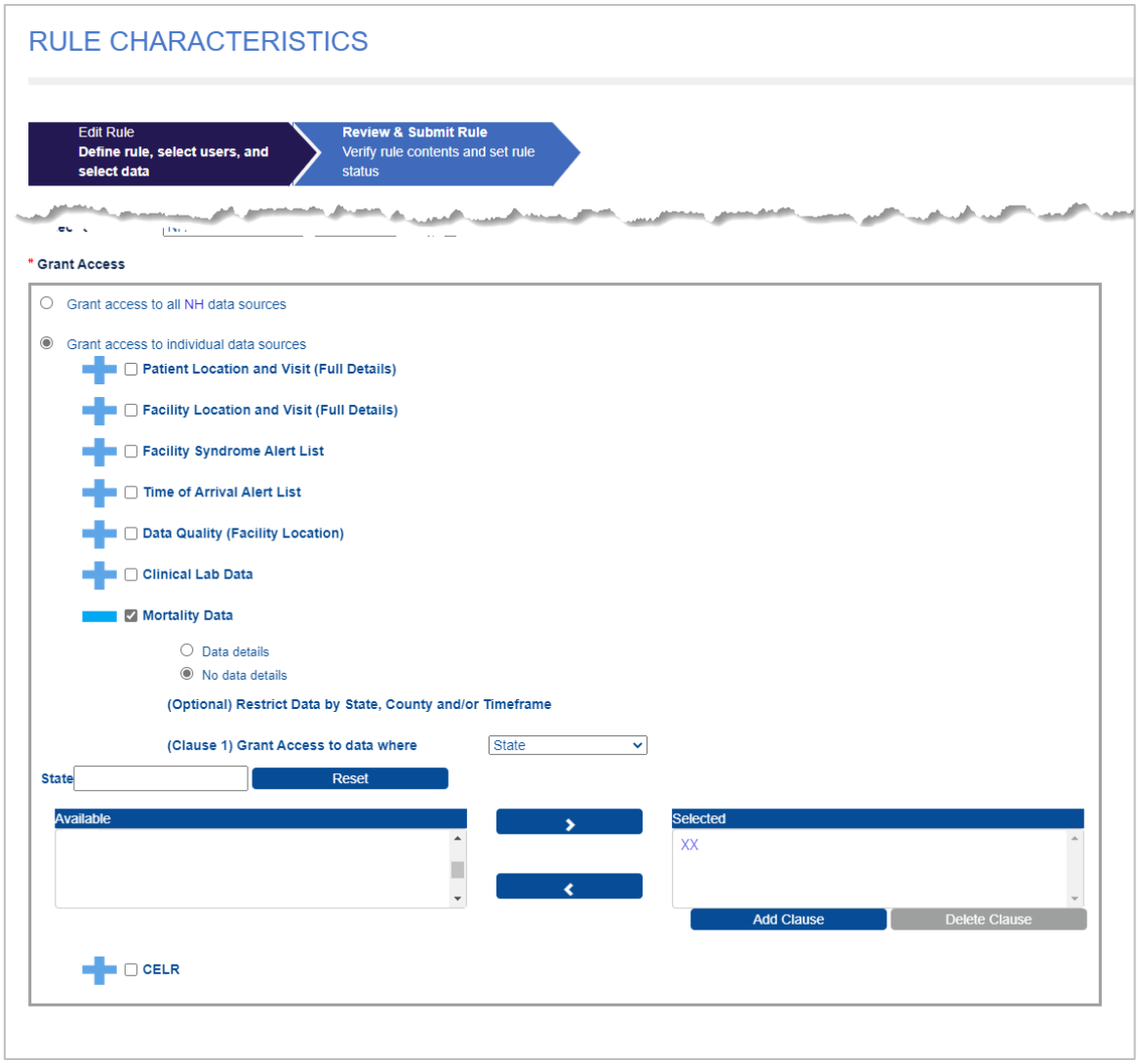


Figure 29. Add New Data Access Rule for Mortality Data

4.3.1.13 Selecting COVID-19 Electronic Laboratory Results (CELR) Data.

The CELR Data Source was added in response to the COVID-19 pandemic of 2020 through 2023. CDC rapidly onboarded health departments to provide timely information on COVID-19 findings using CELR.

By April 21, 2021, 56 jurisdictions had converted to electronic laboratory results reporting, representing 100% of the total laboratory testing volume in the United States.

These data were onboarded to the BioSense Platform and data access rules for CELR are available in AMC. CELR data are available to each site, and access can be assigned using a data access rule. The only parameters for restricting access are Timeframe–From and Timeframe–To dates. Figure 30 illustrates a rule that grants access to CELR data during a prescribed timeframe based on the earlier date in records with both Lab Order Date and Results Date fields populated.

The format for Timeframe–From and Timeframe–To dates is mm-dd-yyyy, or use the popup calendars for dates.

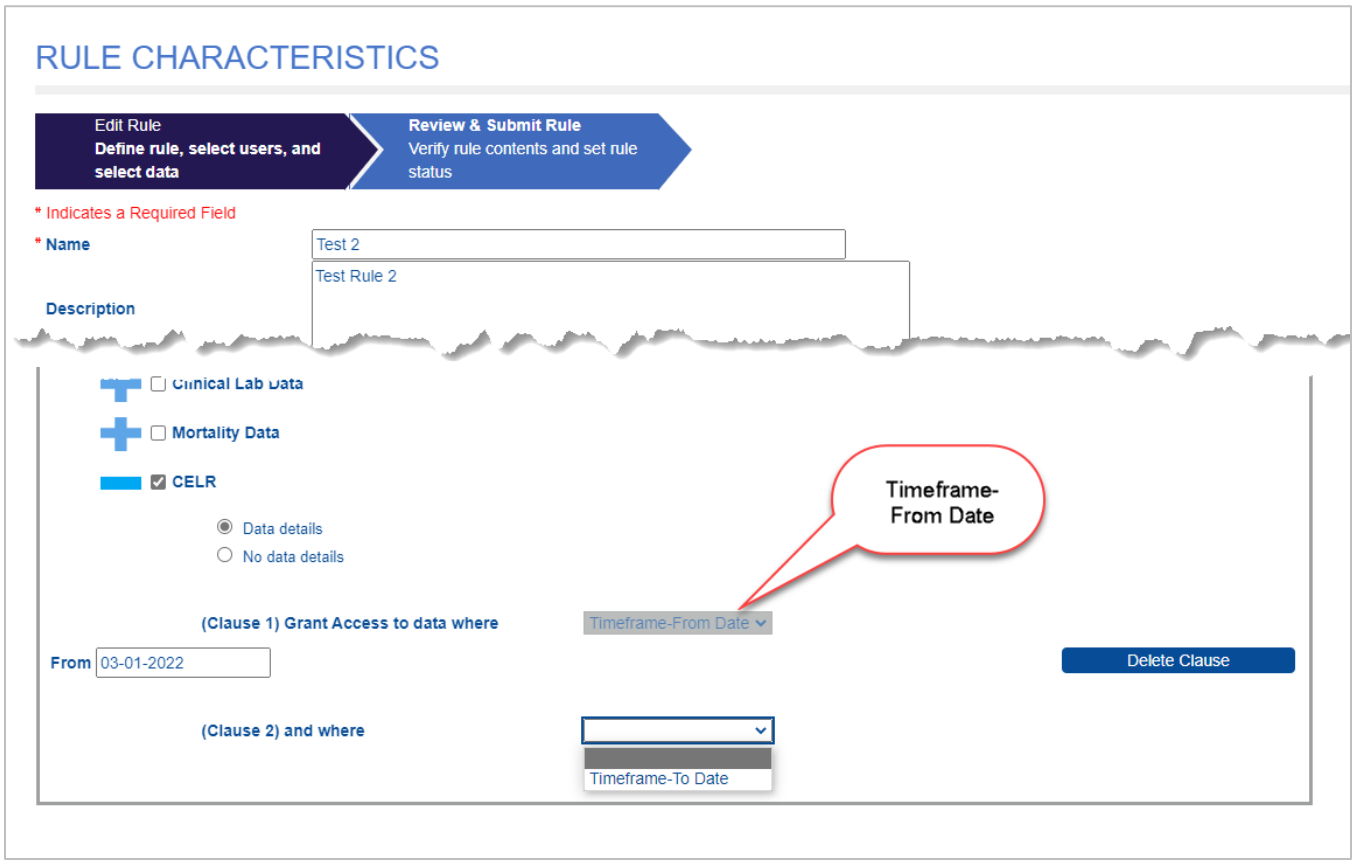


Figure 30. CELR Data Source Timeframe Parameters

4.3.2 Review and Submit the Rule

Once you name your rule and select users and data, you're ready to submit and implement your Data Access Rule. First, confirm that your selections are as expected. If you need to make changes, use the **Back/Edit** button to return to the Edit Rule page. Next, select the appropriate status for your rule (note that the default status value is "Draft"):

Data Access Rule Status

Each status provides the current state of the rule and indicates if the rule is being used in ESSENCE.

- **Draft:** This is the initial status when you first create a rule in AMC. At this point, it has **not** been sent to ESSENCE. If you change its status to *Active* and submit it, it will be sent to and activated in ESSENCE. This will affect the user(s) and groups that you included in the rule.
  Note: A rule's status can also be changed from *Active* to *Draft*. This is equivalent to *Suspend* status in that the rule is removed from ESSENCE but still exists in AMC.
- **Active:** This indicates that the rule has been submitted to ESSENCE and is being used to filter ESSENCE data as specified in the rule's parameters.
- **Delete:** If you change a rule status to *Delete* and submit the change, the rule will be deleted from the AMC and ESSENCE, and the rule will no longer be available.
- **Suspend:** Suspending a rule removes it from ESSENCE but does not delete it from AMC. Functionally, this has the same effect as setting a rule back to *Draft*. However, *Suspend* can be used to indicate that the rule was once an *Active* rule in the system.
  Note: Changing the status from *Active* to *Draft* will have the same result as changing it from *Active* to *Suspend* in that the rule will be removed from ESSENCE but will remain in the AMC. It can be activated from either the *Draft* or *Suspend* state.

When you're done, click the **Submit** button (Figure 31). You'll be returned to the Data Access tab.

After submitting a rule, check with the users or a person within a group of users (if the rule has been created for a group) to find out if they can view the expected data. If they cannot, check the Rule Status. The rule must be Active to be operational in ESSENCE. A rule in Draft or Suspend status is *not active* in ESSENCE.

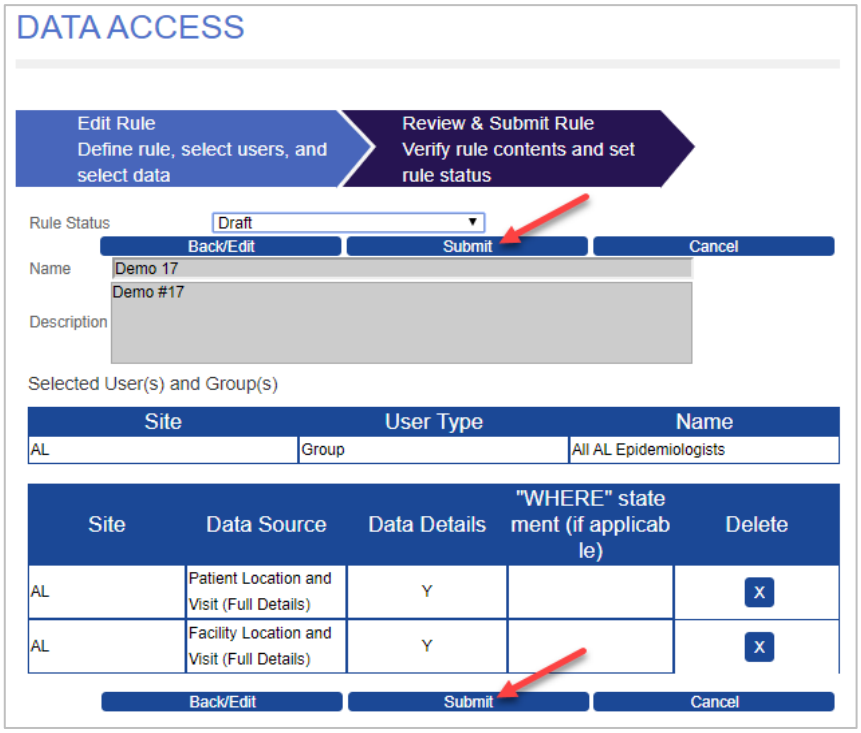


Figure 31. Data Access Page (Review and Submit Rule)

4.3.3 Edit a Data Access Rule

Existing rules can be changed. Just go the Data Access tab and select a rule that you want to change.

4.3.3.1 Select a Rule to Edit

On the Data Access tab, *View and modify existing Data Access Rules* section, click the **View/Edit** button beside the rule you want to edit (Figure 32).

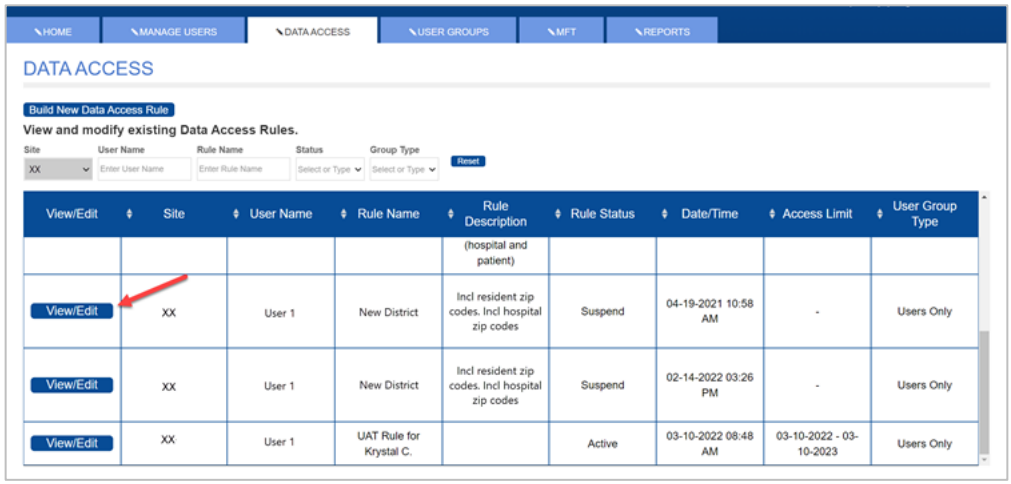


Figure 32. Data Access Page (Editing Rules)

4.3.3.2 Modify Rule Characteristics and Save

After you click **View/Edit**, you'll be directed to the DATA ACCESS > Edit Rule page (Figure 33) where you will click the **Back/Edit** button to modify the rule.

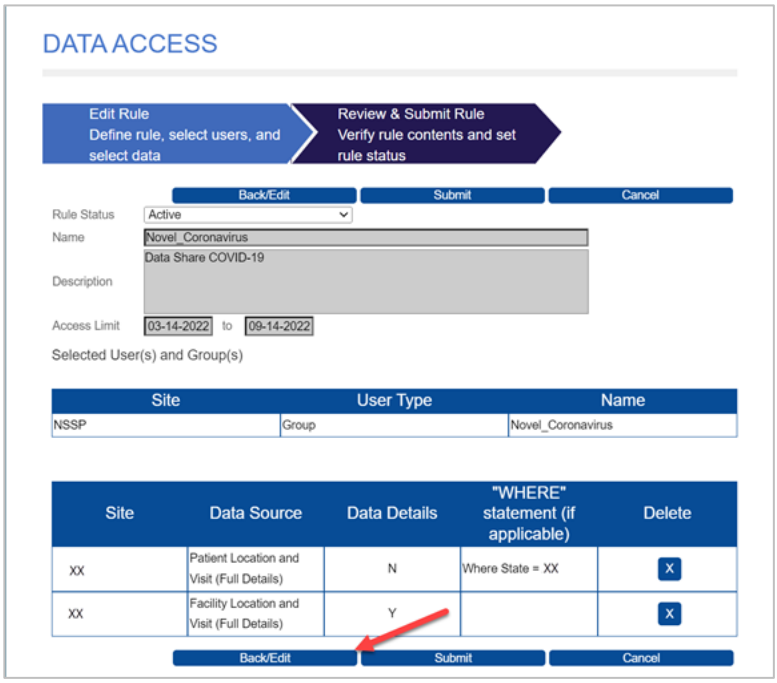


Figure 33. DATA ACCESS > Edit Rule Page

The Back/Edit button will take you to the "Edit Rule" section on the Rule Characteristics page. There you can change the rule name and description; add or delete users and groups; and add, delete, or modify data sources. You can also use the "Rule Status" drop-down list to change a rule's status (for example, from Active to Draft).

In addition, the rule can be deleted entirely by clicking on the **X** in the Delete column.

On this page, you can also modify or delete WHERE clauses. To do this, first expand the Data Source that the WHERE clause is associated with by clicking on the **blue** plus sign (**+**) next to it. The Data Sources details will be displayed (Figure 34).

Here, values from the Available pick list may be added to or Selected values may be removed from the WHERE clause. After changes are completed, click the **Update Clause** button.

You may completely delete this WHERE clause by clicking the **Delete Clause** button.

When you finish modifying your Data Access Rule, click the **Next** or the **Save/Submit** button.

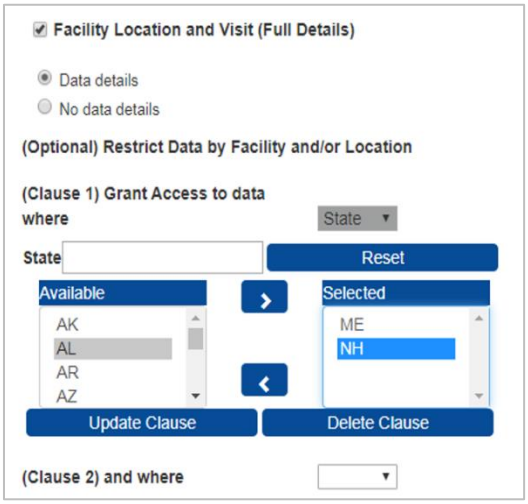


Figure 34. Data Source Details

4.3.3.3 Stop Using a Rule

There are two options when you want to stop using a rule. You may suspend it, which deactivates it but keeps it in the system, or you may delete it, which completely removes it.

Option #1 How to Suspend or Deactivate a Rule

Follow these steps to suspend or deactivate a rule:

1. Select the rule from the Data Access tab and click **View/Edit**.
2. In the Status drop-down list, change the value to "Suspend."
3. Click **Submit**.

Option #2 How to Delete a Rule

Follow these steps to *completely* remove a rule:

1. Select the rule from the Data Access tab and click **View/Edit**.
2. In the Status drop-down list, change the value to "Delete."
3. Click **Submit**.

If you have a rule containing multiple data sources and need to delete an individual data source from that rule, use the **X** button in the Delete column on the Data Access > Edit Rule page (Figure 35).

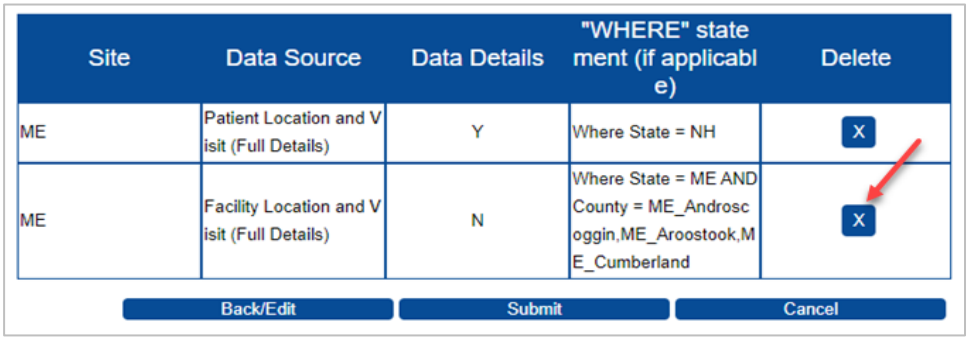


Figure 35. Deleting a Rule for a Single Data Source

Note: If a rule is suspended, the rule will be removed from the user account(s) in ESSENCE. However, the AMC will preserve the Data Access Rule with a status of "Suspend," and you may reactivate it later.

If a rule is deleted in the AMC, it will be removed from both AMC and ESSENCE.

5. Examples of AMC Data Access Rules

The AMC uses rules to control access to ESSENCE data sources, most of which have two access controls: facility location and patient location. Shown below (Figures 36–41) are some typical ways in which rules govern data being shared.

5.1 Facility Location Examples

Selected Data

Site	Data Source	Data Details	"WHERE" statement (if applicable)	Delete
Site Name	Facility Location and Visit (Full Details)	Y		X

Figure 36. A Site Shares "Facility Location and Visit (Full Details)" Data for All Facilities

Selected Data

Site	Data Source	Data Details	"WHERE" statement (if applicable)	Delete
Site Name	Facility Location and Visit (Full Details)	N	Where State = Site AND County = St_Cty	X

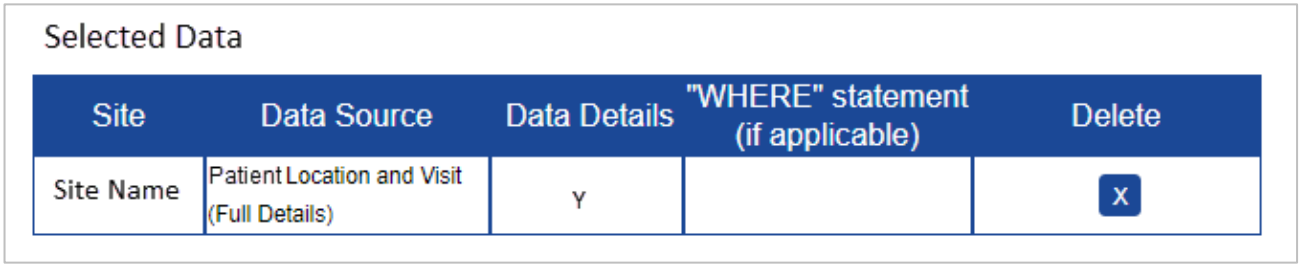
Figure 37. A Site Shares “Facility Location and Visit (Full Details)” Data for a Specific County

Selected Data

Site	Data Source	Data Details	"WHERE" statement (if applicable)	Delete
Site Name	Facility Location and Visit (Full Details)	N	Where State = Site AND Facility = 333	X

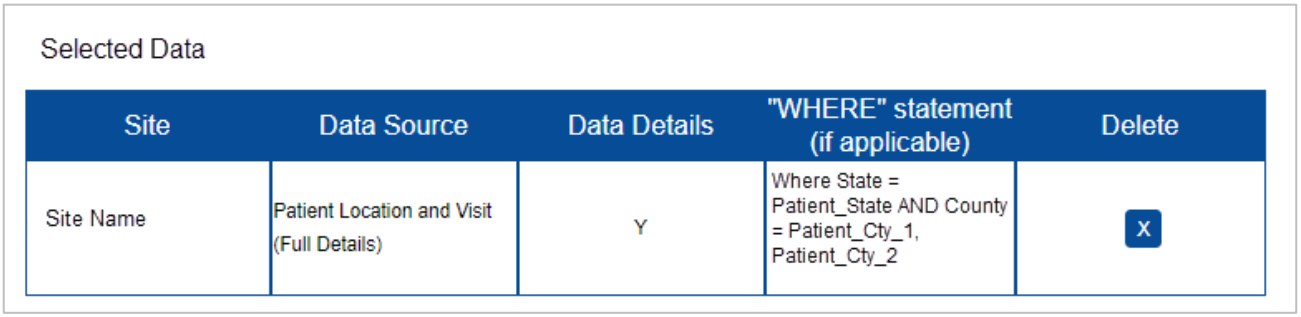
Figure 38. A Site Shares “Facility Location and Visit (Full Details)” Data for a Specific Facility

5.2 Patient Location Examples


Selected Data

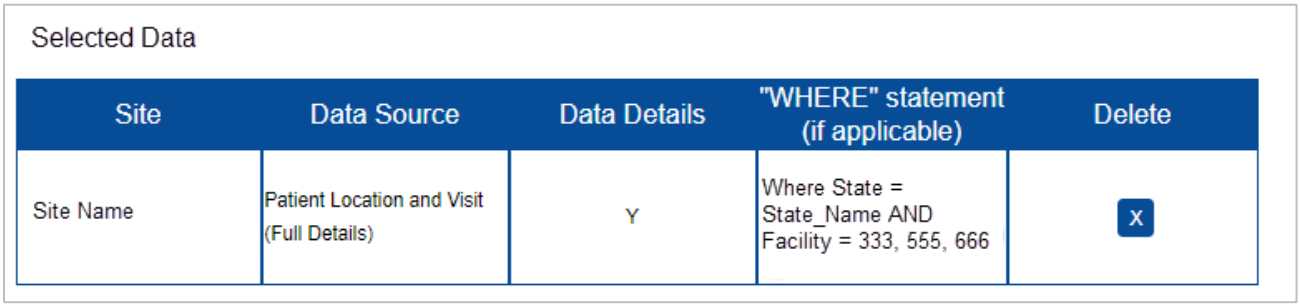
Site	Data Source	Data Details	"WHERE" statement (if applicable)	Delete
Site Name	Patient Location and Visit (Full Details)	Y		X

Figure 39. A Site Shares "Patient Location and Visit (Full Details)" with Data Details for Your Site


Selected Data

Site	Data Source	Data Details	"WHERE" statement (if applicable)	Delete
Site Name	Patient Location and Visit (Full Details)	Y	Where State = Patient_State AND County = Patient_Cty_1, Patient_Cty_2	X

Figure 40. A Site Shares "Patient Location and Visit (Full Details)" Data Where the Patient Lives in a Specific County (based on patient ZIP Code)


Selected Data

Site	Data Source	Data Details	"WHERE" statement (if applicable)	Delete
Site Name	Patient Location and Visit (Full Details)	Y	Where State = State_Name AND Facility = 333, 555, 666	X

Figure 41. A Site Shares "Patient Location and Visit (Full Details)" Data for Facilities 333, 555, and 666 Where the Patient Lives in State "State_Name"

5.3 Sharing County Data with a User in Another State

When data are reported for a patient who resides in another state, those data cannot be viewed by the patient's home state health authorities unless a Data Access Rule is set up to enable data sharing between sites.

For example, a New Hampshire resident who lives in a county bordering Maine is visiting in Maine when an event occurs requiring a visit to a local (Maine) emergency department. This event and others like it may be of interest to New Hampshire state health authorities, but for them to see data for events like this, the Maine site administrator must create a Data Access Rule to share these data.

Below are the steps that the Maine site administrator can take to create a rule to share Patient Location data with New Hampshire:

1. Log in to AMC and select the "Data Access" tab.
2. Click the **Build New Data Access Rule** button.
3. Name the rule and enter a short description.
4. In the "Search for and Select Users or Groups to include in this Data Access Rule" section, click the **blue** plus sign (**+**) to expand the "Select Individual Users" pick list or, if you want to choose a group, click the plus sign (**+**) by "Select a Group" to see the Groups pick list.
5. Scroll down or use the filter fields above the pick list to locate the individual(s) or group(s) in New Hampshire. Highlight those you want to allow to access the data and use the greater than symbol (**>**) to move them to the Selected list. **Note:** Your state (site) will be preselected under the "Select data to include in the data access rule" section.
6. Check the **Grant access to individual data sources** radio button.
7. Click on the checkbox next to the "Patient Location and Visit (Full Access)" source.
8. Next, choose **Data details** or **No data details** radio button for the level of access.
9. In the "(Optional) Restrict Data by Facility, Location, Timeframe and/or Syndrome (ESSENCE Category)" section, choose the "(Clause 1) Grant Access to data where" drop-down list and select **State** (Figure 42).

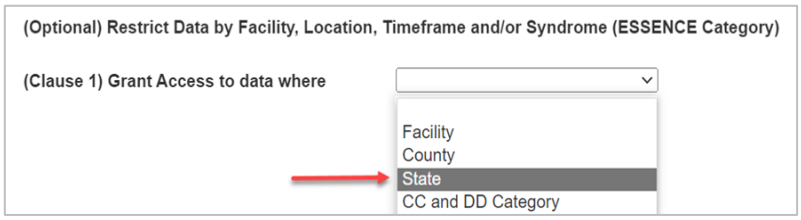


Figure 42. Select State from Clause 1 Drop-down List

When you select State, the State pick list is displayed (Figure 43):

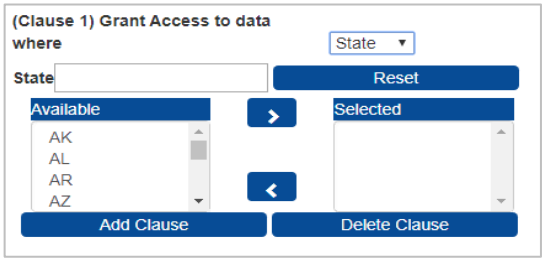


Figure 43. State Pick List

10. Using the “Available” pick list or using the “State” search field above it, highlight the state (site) for which you want to share patient data (New Hampshire) and, using the greater than symbol (**>**), move the state abbreviation (NH) to the “Selected” list, then click the **Add Clause** button. When you do, you will be given an input drop-down for a second WHERE clause.
11. If you want to limit the counties they can access, then use “Clause 2” and select “County” from the input drop-down. This will display all the counties in New Hampshire (the state for which you want to share data). They will be displayed in the “Available” pick list. Highlight the counties for which you want to grant data access, and then use the greater than symbol **(>)** to move them to the “Selected” pick list.

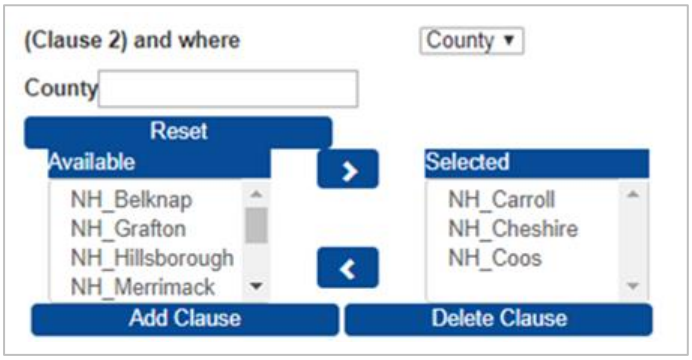


Figure 44. Chosen Counties Moved to Selected Pick List

12. Once you have moved these counties to the “Selected” pick list, click the **Add Clause** button. This will create the WHERE Clause to grant the data access (for example, *Where State = NH AND County = NH_Carroll, NH_Cheshire, NH_Coos*). Save this rule by using the **Next** or **Save Draft** button. The **Cancel** button is also available here in case you decide to abandon your work on this rule.

    The difference between **Next** and **Save Draft** is that **Next** takes you to the Review and Submit Rule page, whereas the **Save Draft** button simply saves your work and returns you to the View and Modify Existing Data Access Rules page where all your rules are listed.

Do’s and Don’ts of Sharing Patient Location and Visit Data

1. You *can* share data with other users in your site and restrict by a patient’s location using the “Patient Location and Visit” data source.
2. When sharing data with users outside your site, we recommend you *do not* share by patient location because ESSENCE will consolidate that rule with other patient location access controls, and you might share more than intended (for details, see the section titled Translate AMC Data Access Rules to ESSENCE).

When satisfied, set the rule to Active and click the **Submit** button (Figure 45). The user or users assigned to this access rule will be able to view the data in ESSENCE based on the data source and data level in the county or counties you selected.

Before activating the rule, confirm that your selections are as expected. Use the **Back/Edit** button to modify the information displayed. Next, **select the appropriate status for your rule** (the default status value is "Draft"):

- Active = rule will be saved and applied
- Draft = rule will be saved but not applied (Draft Status)
- Suspend = rule will be saved but not applied

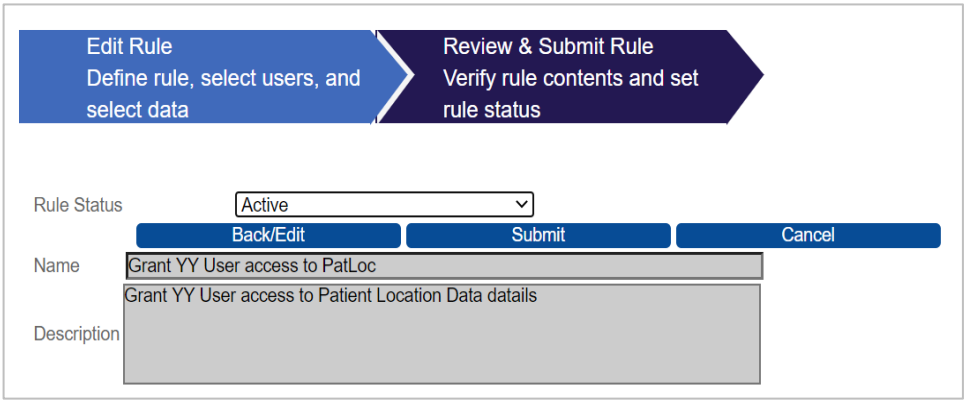


Figure 45. Data Access Page (Review & Submit Rule)

When you're done, click **Submit**. You'll be returned to the Data Access tab.

5.4 Example—Editing a Rule

Step 1: Select a Rule

On the Data Access tab under View and modify existing Data Access Rules, click the **View/Edit** button beside the rule you want to edit (Figure 46).

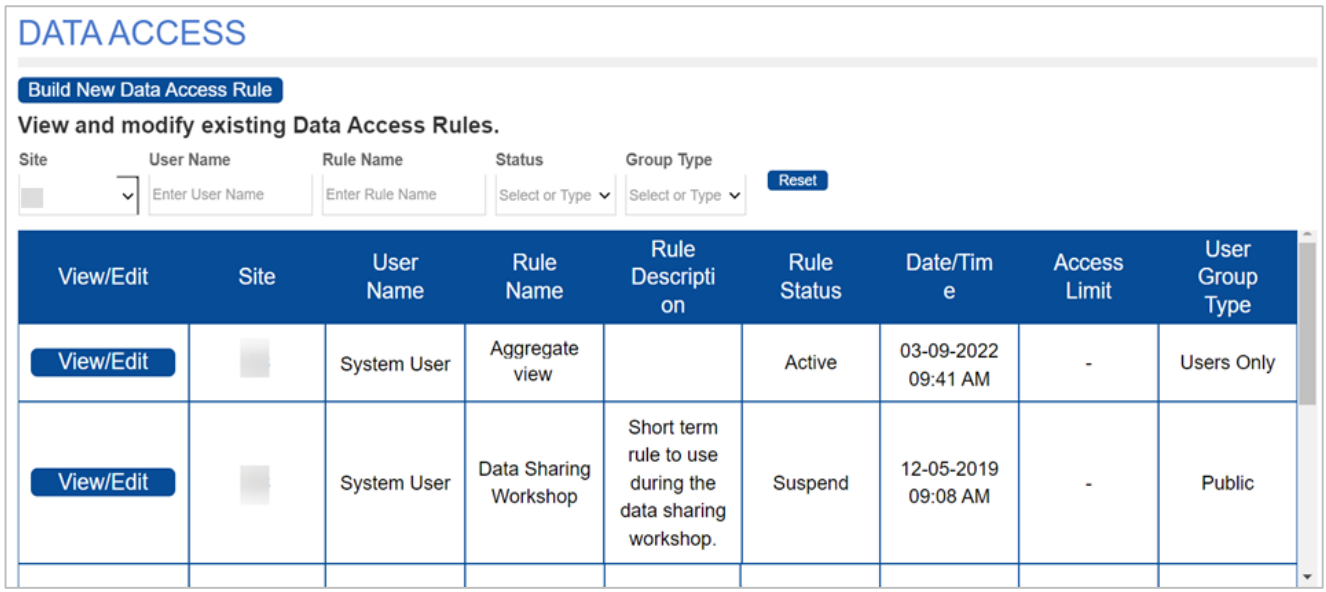


Figure 46. Data Access Page (Editing Rules)

Step 2: Modify Rule Characteristics and Save

After you click **View/Edit**, you'll be directed to the Review & Save page (Figure 47). Use the "Edit" buttons to change rule information, users, or data. You can also use the status drop-down list to change a rule's status. When you finish modifying your Data Access Rule, click **Submit**.

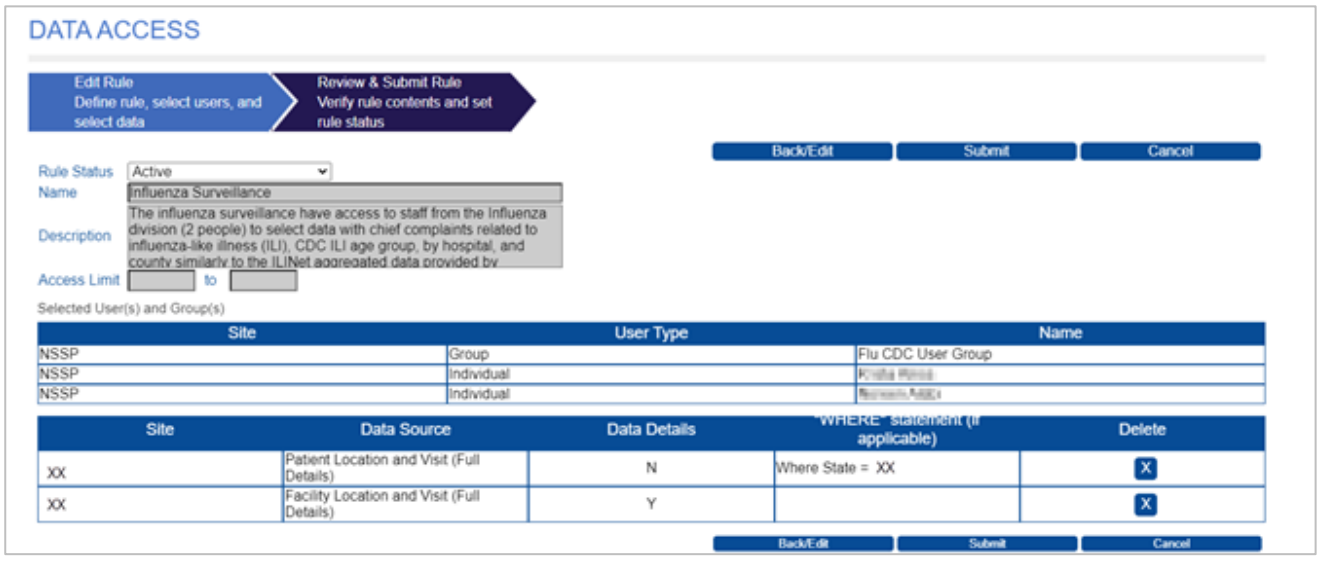


Figure 47. Editing Rules (Review & Save)

5.5 Translate AMC Data Access Rules to ESSENCE

The AMC uses rules to control access to ESSENCE data sources. Most ESSENCE data sources have two access controls: Patient Location and Facility Location.

Suppose you want to share the "Patient Location and View (Full Details)" data source for your site. You can use the AMC to create a Data Access Rule to share all your site's data for the "Patient Location and View (Full Details)" data source. The AMC will translate these selections into ESSENCE as demonstrated in the table below.

I want to…	Site	State	County	Data source *(ESSENCE Variable Name)*	Facility
Share all the data from my site	;SiteID;	*	*	;va_e54esrdfxfr_hosp;	*
For patients that live anywhere (but were seen in my site)	*	*	*	;va_er;	*

ESSENCE manages data access for each user account by consolidating all data selected in rules that include that user and assigns the highest level of access for any given data source.

Suppose you want to share data from your site, Site X (where the patient lives in Alaska), with another user, John Doe. John already has access to all data by patient location for a different site, Site Y. His current data access at Site Y would be as follows:

John Doe can access…	Site	State	County	Data source *(ESSENCE Variable Name)*	Facility
All data from site Y	;SiteY ID;	All	All	;va_er_hosp;	All
For patients that live anywhere (but were seen in site Y)	All	All	All	;va_er;	All

Your rule in the AMC to share your site's data by patient location of Alaska would be as demonstrated below:

Your rule grants access to…	Site	State	County	Data source *(ESSENCE Variable Name)*	Facility
All data from site X	; SiteX ID;	All	All	;va_er_hosp;	All
For patients that live in Alaska (but were seen in site X)	All	Alaska	All	;va_er;	All

If you include John in your rule, he will be able to access *all your site's data* because **ESSENCE combines data access and defaults to the highest permission available** for the "Patient Location (Full Details)" data source. John's combined data access would be:

John's access after the rule…	**Site**	**State**	**County**	**Data source** ***(ESSENCE Variable Name)***	Facility
All data from these sites	;SiteX ID; SiteY ID;	**All**	All	;va_er_hosp;	All
For patients that live in Alaska	All	**All** ~~Alaska~~	All	;va_er;	All

6. User Groups

User groups are a convenient way to add multiple users to data access rules instead of having to add individual users one-by-one. For example, you could create a data access rule for all your epidemiologists to provide access to data they might want to use. Instead of adding each epidemiologist to that rule, just add the "All Epidemiologists" user group. If all epidemiologists in your site have the Epidemiologist checkbox selected in their user profiles, then they will appear in your All Epidemiologists user group.

The User Groups tab is only available to site administrators and superusers (Figure 48). Displayed on the Manage User Groups page are an **Add New User Group** button, the My Site User Groups table, the Download User Groups Report generator with a **Download Report** button, and the All Public User Groups table.

Directly above each table are dynamic (free text) search filters for Name and Description. Filters for Site and Type, also located here, are triggered by selecting a value from their drop-down lists.

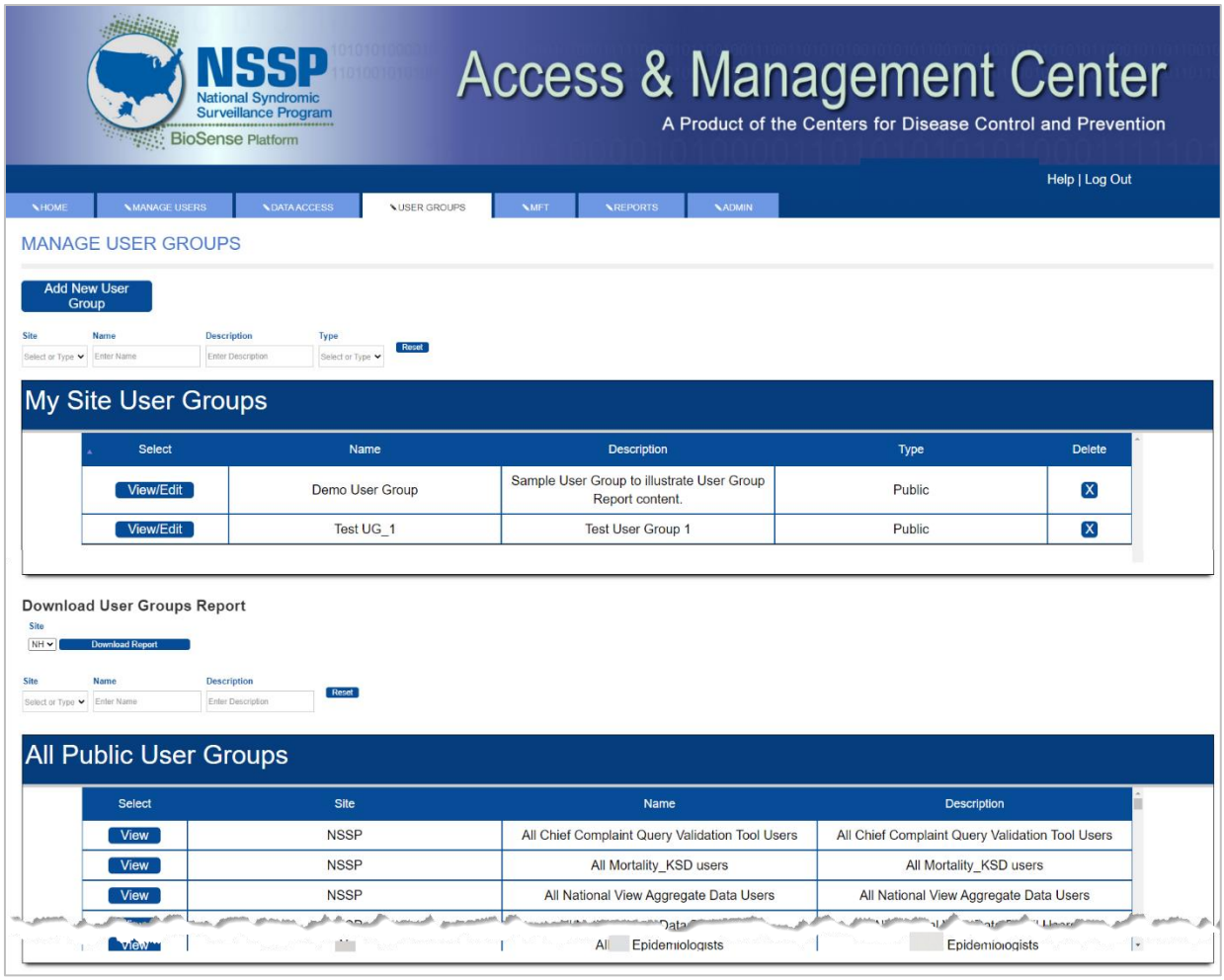


Figure 48. User Groups Page—View/Edit My Site User Groups—View Public User Groups

Here are the search parameters that can be used:

- Site—[Drop-down List] For site administrators, your site is the only site presented.
- Name—[Free-text Field] This is used to search for group names.
- Description—[Free-text Field] This is used to search for group descriptions.
- Type—[Drop-down List] The Type field is only available on the My Site User Groups table. The types, *Private* or *Public*, can be selected from this field's drop-down list.

Note: Entering characters in free-text fields will trigger dynamic string searches. For example, "Gr" and "ou" will both find the word "group" in either upper or lower case. These dynamic searches begin when the first character is entered, so occasionally you may experience a short delay as you begin entering a search string.

There two types of user groups, *Public* and *Private*:

- *Public* user groups are viewable and usable by all other site administrator and superusers to add to data access rules they create or administer.

  Public user groups may appear in two tables on the Users Groups page. My Site User Groups table lists all (*Public* and *Private*) user groups created in your site and can be viewed or modified by clicking on the **View/Edit** button, then the **Back/Edit** button. New users can also be added to a group when on the View/Edit page by clicking on the small **Add/Edit User** button below the View & Select Users—Users assigned to current Group table.
- *Private* user groups are only viewable and usable by the site's administrators or superusers but can only be assigned to your site's data access rules in the same way as *Public* user groups.

Site administrators and superusers may create any number of *Public* or *Private* user groups.

There are two *Public* user groups that are created automatically:

- All [*site name*] Users
- All [*site name*] Epidemiologists

New users are added to the *All [site name] Users* group when they are created and, if the **Epidemiologist** checkbox is marked on their User Profile, they are also added to the *All [site name] Epidemiologists* group. These two groups appear in the All Public User Groups table for every site in the BioSense Platform.

There is also functionality to download your User Groups Report. The **Download Report** button generates a CSV-formatted report listing all your site's User Groups and their associated users. **Note:** Superusers may select any site from the Site drop-down list, whereas site administrators are limited to user groups for their site.

Once a user group is created, it can be assigned to any data access rule within your site. *Public* user groups are accessible to other sites, and they may use them to grant your users access to their data sources by adding one or more of your *Public* user groups to their data access rules.

> Keep in mind that individual users can be added to a user group or directly to a Data Access Rule by using the checkboxes at the bottom of the User Profile page as referenced in Section 4.2.3.

6.1 Create a New User Group

Step 1: Select User Group Characteristics

Click the **Add New User Group** button on the User Groups Characteristics page. Enter the user group's characteristics (Figure 49): Create a unique name for the user group, add a description, and select a type (*Public* or *Private*) for the group.

We recommend that you provide enough detail in the Description field to enable you to quickly distinguish what this user group is for. Note that the Site field will show the logged-in administrator's site and cannot be changed.

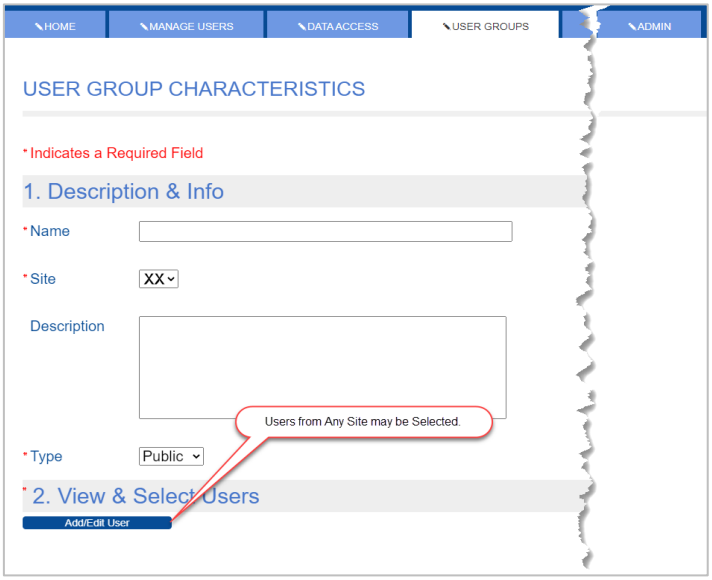


Figure 49. Add New User Group

Group Types: There are two types of groups:

- ***Public***—Anyone authorized to manage user groups (typically site administrators and superusers) can see the *Public* groups in all sites. These are listed in the All *Public* User Groups table on each site's Manager User Groups page. When creating a *Public* user group that another site might use, consider including your site's abbreviation or short name in these *Public* user groups' names. This naming convention will make for easier identification when numerous sites' user groups have been added to another site's data access rule. **Note:** *Public* is the default group type.
- ***Private***—Only site administrators who are associated with the site that owns and controls private groups will see these user groups.

Step 2: Select Users

Click the **Add/Edit User** button to add users to the group (Figure 50). At least one user or group must be selected to create a group. Remember that any users selected here will receive access to the data you specify in your data access rule when you add this new group to the rule.

Use the filters to locate users to add to the group. Add users by clicking the **Add** button next to the user's name. When you've finished adding users, click the **Submit** button at the bottom to save the group. Once saved, your group is active and can be used.

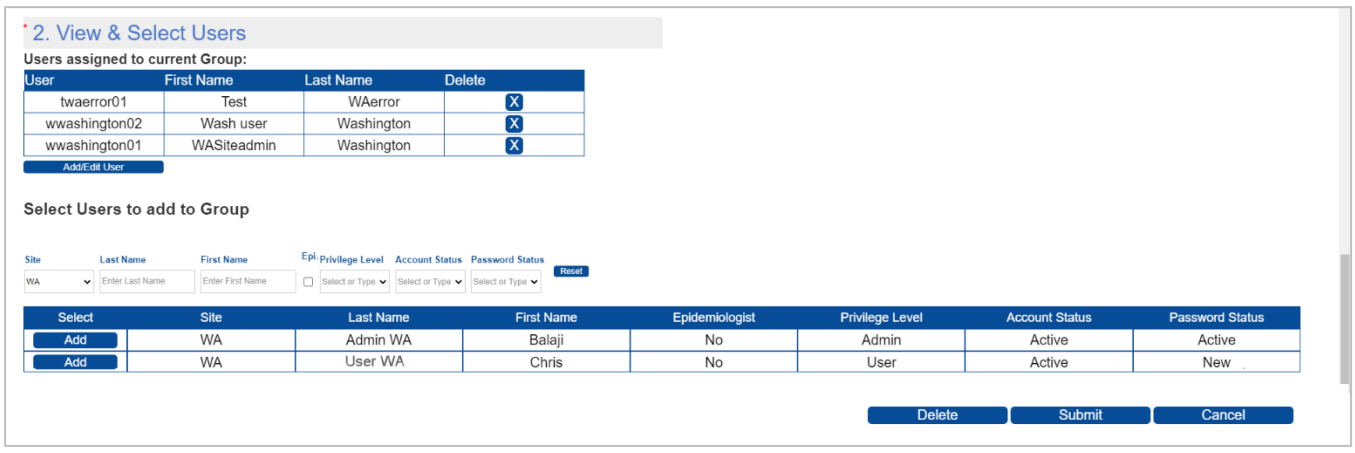


Figure 50. User Groups Page (Select Users and Submit)

6.2 Edit a User Group

Site administrators may edit the user groups that have been created for their site, in other words, the groups that are listed in their My Site User Groups table. Examples include changing the group name, changing the group to *Public* or *Private*, and adding or removing group members. The site administrator may also delete a group that is no longer needed.

Once a user group is associated with a data access rule, the site administrator may delete or add users without affecting other group members. The remaining members of the user group will maintain their association with the user group's previously assigned data rules.

Membership of a user group provides access to ESSENCE syndromic surveillance data only if:

- The user group is assigned to one or more access rules allowing access to ESSENCE.

Additionally, a member of a user group can access ESSENCE syndromic surveillance data if:

- The member is also assigned to one or more different user groups that have been assigned to a rule allowing access to ESSENCE, or
- The member has been individually assigned to an access rule allowing access to ESSENCE.

In other words, a user group can provide access by being directly assigned to an access rule that provides such access or by having a group member who already has access by another access rule.

6.3 Delete a User Group

Site administrators may delete a user group that was created in their site. Figure 51 illustrates this procedure.

Just click on the X (1) at the right end of the row describing the user group that you want to delete and, when the "Delete User Group" dialog box pops up, click on the Delete (2) button.

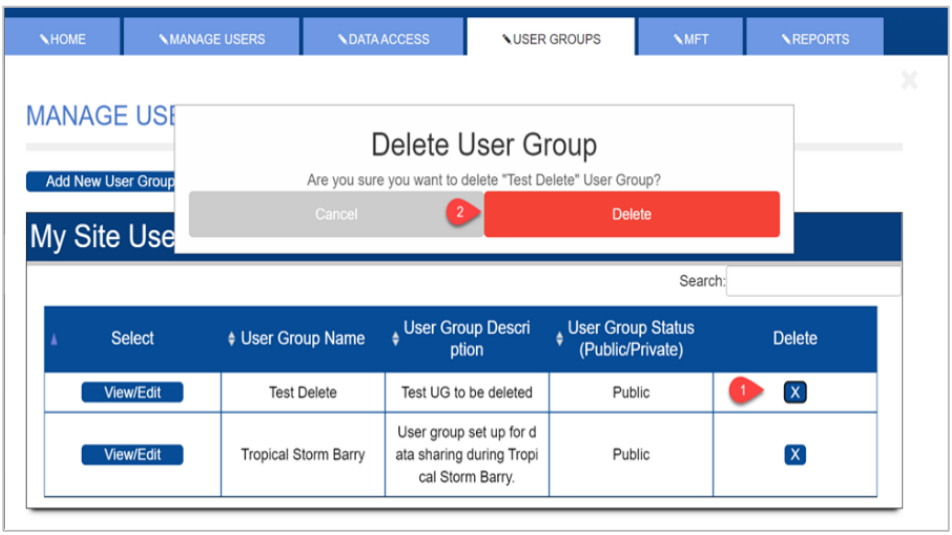


Figure 51. Deleting a User Group

7. Master Facility Table

The Master Facility Table (MFT) resides within the AMC and provides an interface for site administrators, users with MFT privileges, and the NSSP onboarding staff to use throughout the multistage onboarding process. Two additional privilege designations are available to extend limited access to other users: **MFT View Only** and **MFT View/Edit**. Both designations provide access to MFT data.

For in-depth instructions, the *BioSense Platform Quick Start Guide to Using the Master Facility Table* can be accessed by clicking the link or clicking the button shown in the red box in the upper right-hand corner of the Master Facility Table (MFT) page (Figure 52).

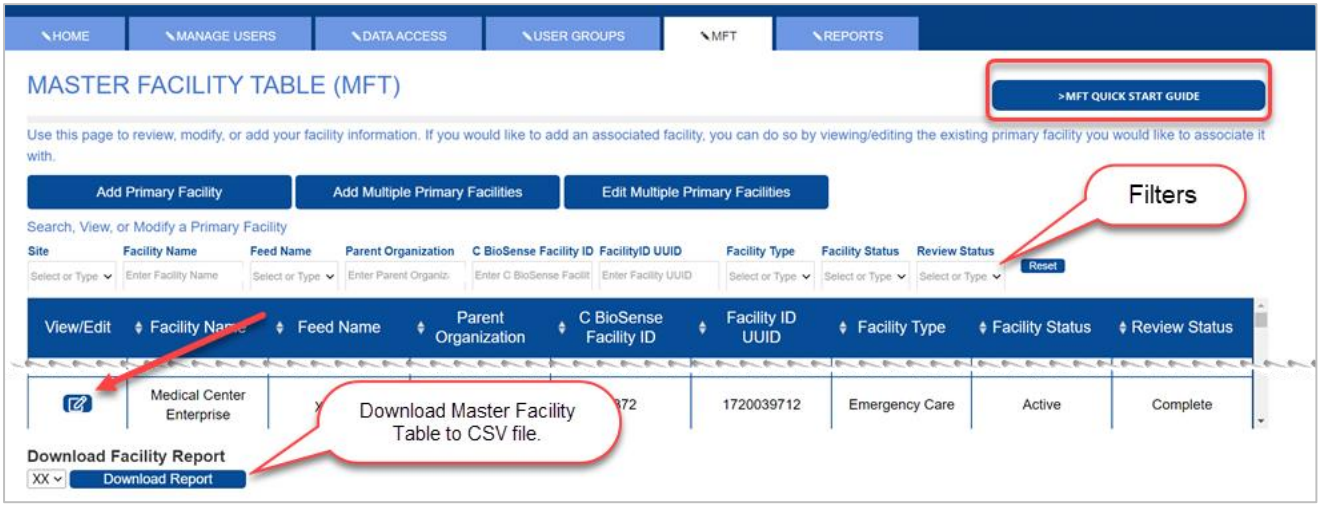


Figure 52. Master Facility Table (MFT) Page

The MFT search fields are a combination of drop-down lists and free-text fields. Because the filters are dynamic, when any criterium is entered, either using one of the drop-down lists or by typing into a free-text field, the search for qualifying facilities begins immediately. This can sometimes cause a slight delay as the search algorithm engages.

Once the table of facilities is populated, any facility in the table can be viewed or edited by clicking on the **View/Edit** button in the first column pointed to by the **red** arrow in Figure 52. More information on functionality follows, but you can also click on the **MFT Quick Start Guide** button in the upper right for in-depth information.

7.1 Add Multiple Primary Facilities

Site administrators and users with MFT View/Edit privileges can add multiple primary facilities to the MFT by selecting the **Add Multiple Primary Facilities** button (Figure 53). The page displayed when you select this button includes instructions on uploading multiple primary facilities and a link to the downloadable template.

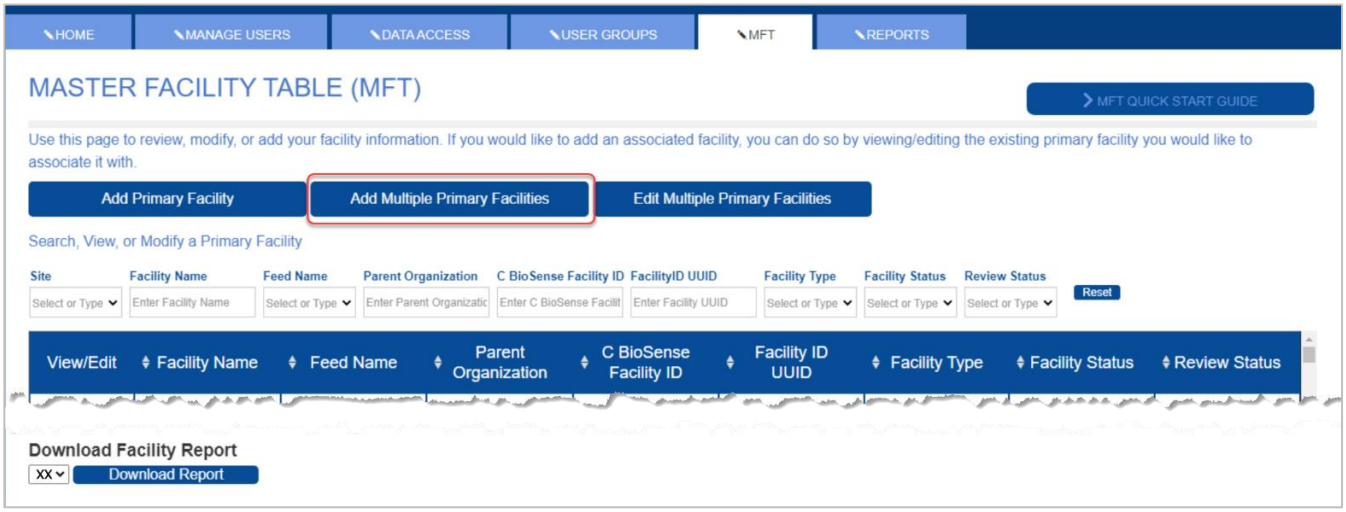


Figure 53. Add Multiple Primary Facilities Button

Click the **here** button as annotated in Figure 54 to download the data input template. Once the downloaded template has been filled in with the required information (see *BioSense Platform Quick Start Guide to Using the Master Facility Table* for details), return to Add Multiple Primary Facilities instructions page (Figure 53) and select the **Browse** button to search for and upload the completed template. When the template is successfully uploaded and verified, click the **Submit** button to process the information.

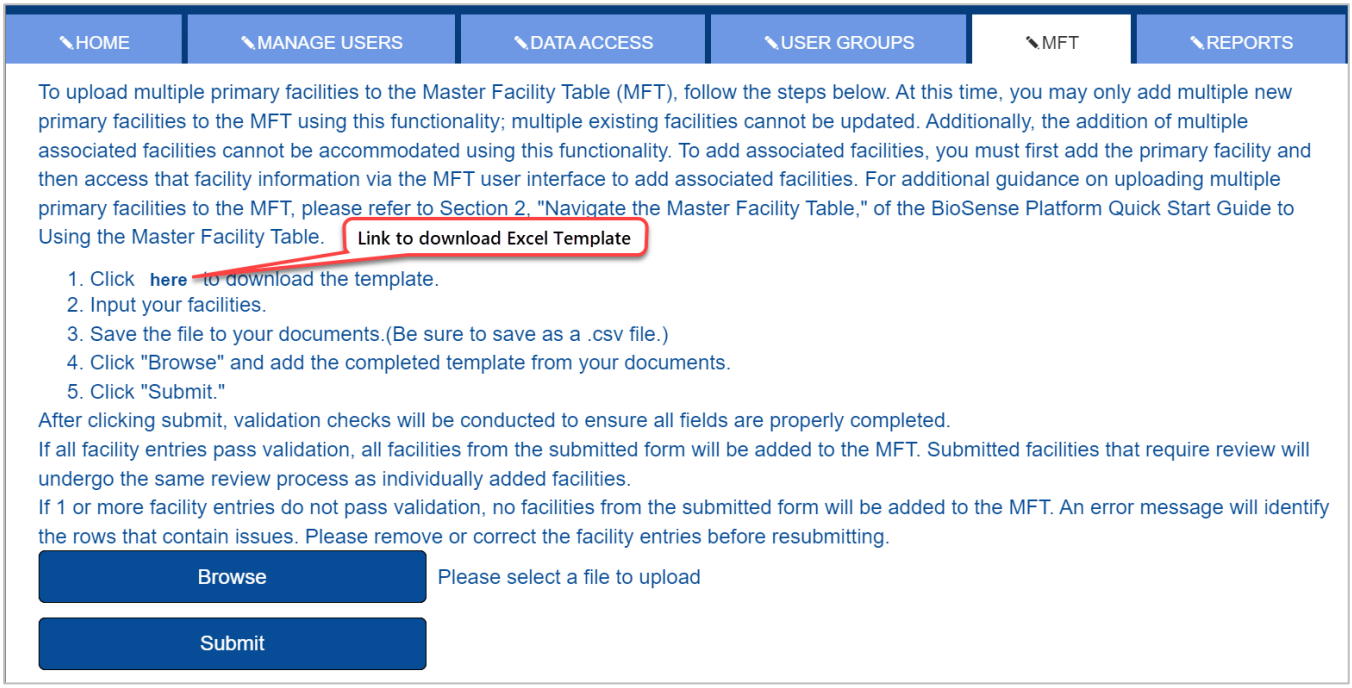


Figure 54. Add Multiple Primary Facilities Instructions (with link)

7.2 Edit Multiple Primary Facilities

Site administrators, superusers, and users with MFT View/Edit privileges can also edit multiple primary facilities by selecting **Edit Multiple Primary Facilities** button (Figure 55). When you click **Edit Multiple Primary Facilities**, the page displays instructions on how to select, download, edit, and then upload primary facilities. To accomplish this, the page will display a table that lists all primary facilities in your site with a checkbox on each row. Use these checkboxes to select the desired facilities to edit.

Once facilities are selected, click **Download Facilities**; this will generate a CSV file and download it to your *Download* folder. Next, update the prepopulated Excel template you have downloaded. Once your updates are made, save the file, and use **Browse** and **Submit** to upload this file.

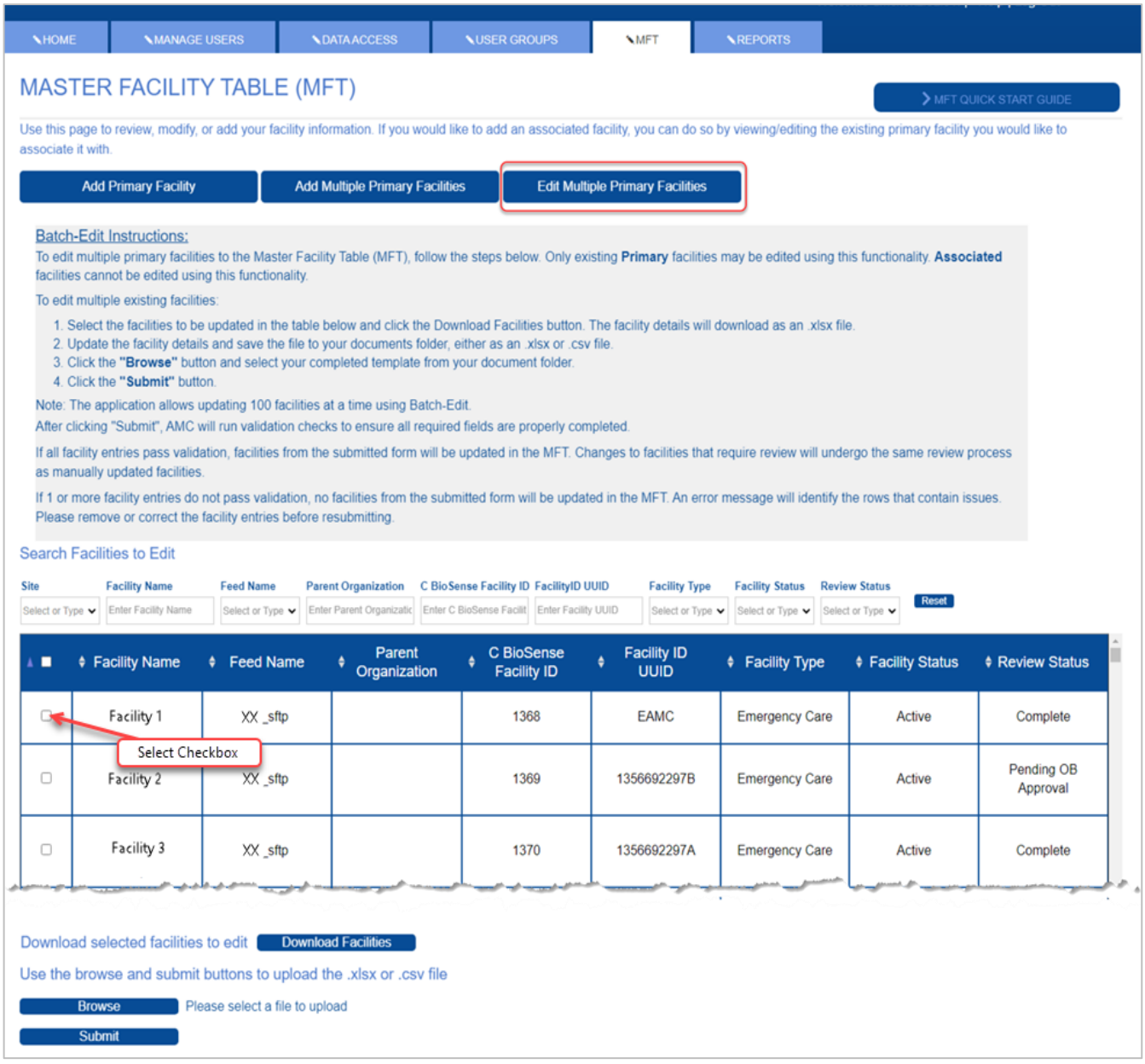


Figure 55. Edit Multiple Primary Facilities Instructions and Selection Screen

7.3 Facility Inactivation Reason and Date

The options for making facilities inactive have been standardized by adding drop-down lists for Reason For Inactivation and the Date Inactivated fields (Figure 56). In the past, this was handled with informal notes in the Facility Status section on the MFT Review page. The standardized inactivation reasons are as follows:

- Closed
- Merged
- 90-day Inactive
- Temporary
- Voluntary

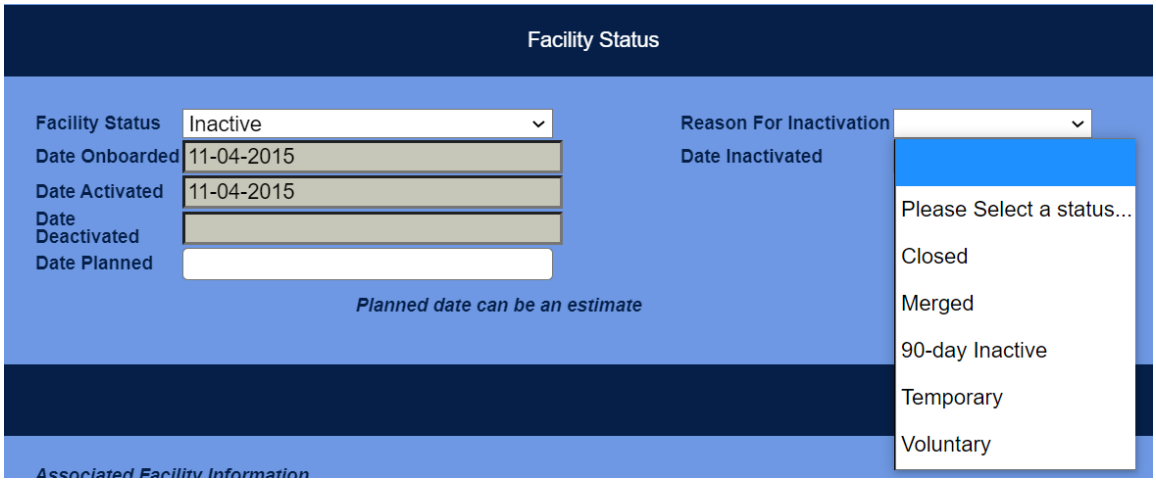


Figure 56. When the facility status is changed to Inactive, the Reason for Inactivation drop-down list becomes available.

Notes:

1. The Reason For Inactivation and the Date Inactivated fields are unavailable until the Facility Status field is set to Inactive.
2. Both the Reason For Inactivation and the Date Inactivated fields become active and are required when the Facility Status is set to Inactive.
3. You may review an old MFT record that is already in an Inactive state; but if you attempt to save it, you will be required to provide the inactivation reason and date. You may click **Cancel**, in which case, no further action will be required.

7.4 Facilities in U.S. Territories

Facilities in U.S. territories can now be added to the Master Facility Table. A list of territories and minor outlying islands are available in the "State" drop-down list. Judicial subdivisions appear in the County drop-down list after the territory or minor outlying island group is selected.

Table 5 shows territories with their "State" abbreviations:

Table 5. U.S. Territory State Abbreviations

U.S. Territory	State Abbreviation
American Samoa	AS
Baker Island	BI
Federated States of Micronesia	FM
Guam	GU
Howland Island	XH
Jarvis Island	JI
Johnson Atoll	JA
Kingman Reef	KR
Midway Islands	QM
Navassa Island	NI
Northern Mariana Islands	MP
Other	OT
Palmyra Atoll	XL
Puerto Rico	PR
Republic of Palau	PW
Republic of the Marshall Islands	MH
U.S. Minor Outlying Islands	UM
U.S. Virgin Islands	VI
Wake Island	QW

Once the State field is populated, the County drop-down will automatically provide associated counties or judicial subdivisions so that those can be designated, if desired.

7.5 Download Facility Report

The **Download Report** button in the lower left can be used to create a full report of all records in the Master Facility Table. Clicking on the **Download Report** button generates a comma separated values (CSV) file then automatically downloads it to your browser's *Downloads* folder (Figure 57).

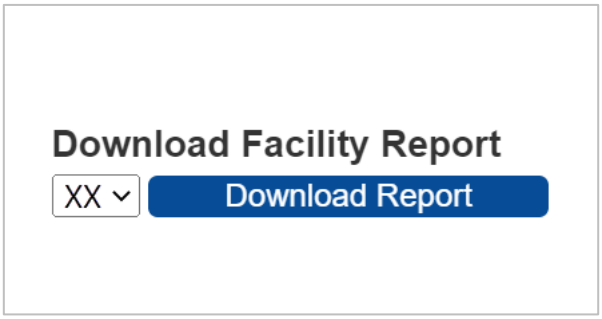


Figure 57. Download Facility Report

The file is named:

Facility_<your AMC user name>_<your site's short_name>_yyyy-mm-dd.

For example, *Facility _xxxxxxxx01_SS_2023-06-15*.csv where *SS* equals your site's short abbreviation.

This file contains all the values for each facility stored in your site's MFT. Currently, there are 61 columns in this file.

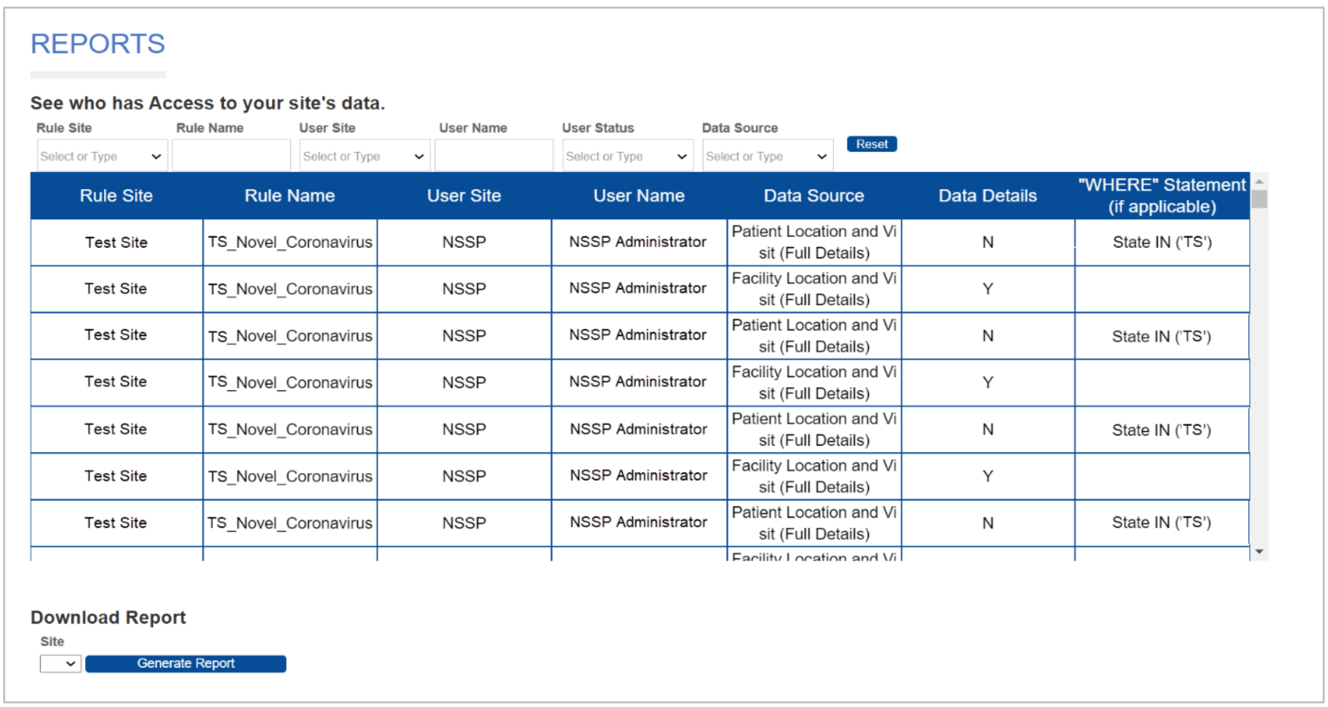
8. Reports

The Reports tab (Figure 58) is only available to site administrators and superusers. This tab provides a table of all the data access rules that affect your site's users and the users in other sites who have been granted access to your site's data.

The table displays the rule site and name, the user's site, and ID with the name of the user granted access, the data source the rule affects, whether data details are available to the user, and any applicable access restrictions (i.e., "WHERE" clauses) included in each rule.

> **Hint**: Sometimes a long time is needed to generate the table on this page, and you may notice that, while the report is being generated, the filter fields are greyed out. When report generation is complete, the filter fields will clear, and you will note that several will contain the instruction "Select or Type."

The table may take several seconds to fully load. Please be patient.



Rule Site	Rule Name	User Site	User Name	Data Source	Data Details	"WHERE" Statement (if applicable)
Test Site	TS_Novel_Coronavirus	NSSP	NSSP Administrator	Patient Location and Visit (Full Details)	N	State IN ('TS')
Test Site	TS_Novel_Coronavirus	NSSP	NSSP Administrator	Facility Location and Visit (Full Details)	Y	
Test Site	TS_Novel_Coronavirus	NSSP	NSSP Administrator	Patient Location and Visit (Full Details)	N	State IN ('TS')
Test Site	TS_Novel_Coronavirus	NSSP	NSSP Administrator	Facility Location and Visit (Full Details)	Y	
Test Site	TS_Novel_Coronavirus	NSSP	NSSP Administrator	Patient Location and Visit (Full Details)	N	State IN ('TS')
Test Site	TS_Novel_Coronavirus	NSSP	NSSP Administrator	Facility Location and Visit (Full Details)	Y	
Test Site	TS_Novel_Coronavirus	NSSP	NSSP Administrator	Patient Location and Visit (Full Details)	N	State IN ('TS')

Figure 58. Data Access Reports Page

The Reports table includes filters for the following report values:

- Rule Site—Allows site administrators to only select their own site and filter out operational access and NSSP rules
- Rule Name—Selects results when a rule name is entered *
- User Site—Selects the site whose user(s) have been granted access
- User Name—Selects a user ID to see the access the user is allowed *

- User Status—Selects only Active or Inactive users
- Data Source—Selects a single Data Source

* The “Name” fields invoke a dynamic pattern-matching search so that you can find occurrences of the characters you type anywhere within the name field. For example: If some User Name fields contain “abudy09 (Alicia Budy)” and others contain “awend01 (Alice Wend)” and you enter “alic” in the User Name search field, all rules for both these users will be displayed.

A full report is available as a CSV file. The file contains all operational access and NSSP rules for the BioSense Platform as well as all rules that grant access to your site’s data sources. This file can easily be viewed in Excel or another spreadsheet application.

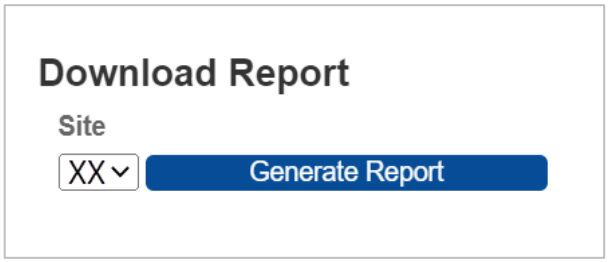


Figure 59. Data Access Reports Page—Generate Report

The **Generate Report** button in the lower left of the Reports page (Figure 59) has a Site selection drop-down list with your site as default. Because site administrators only have access to their site, their Site drop-down list only contains their site.

Click the **Generate Report** button to download a CSV file containing it to your browser’s default download folder. After a few moments, you may directly access the file in your Download folder using Excel or other similar program.

The file is named:

Report_<your AMC user name>_<your site’s short_name>_yyyy-mm-dd.csv
For example, *Report _dmacCando01_SS_*2023-06-15.csv where *SS* equals your site’s short abbreviation.

9. Admin Tab

The Admin tab provides the site administrators and superusers with access to administrative reports and other functionality. Currently, site administrators only have access to the Software Usage information for their site. As described later, additional functionality is available to superusers.

9.1 Site Administrator View

Currently, the site administrator's view of Software Usage (Figure 60) is exclusively for Posit (RStudio) Workbench.

In the future, we plan to track SAS Studio usage, as well.

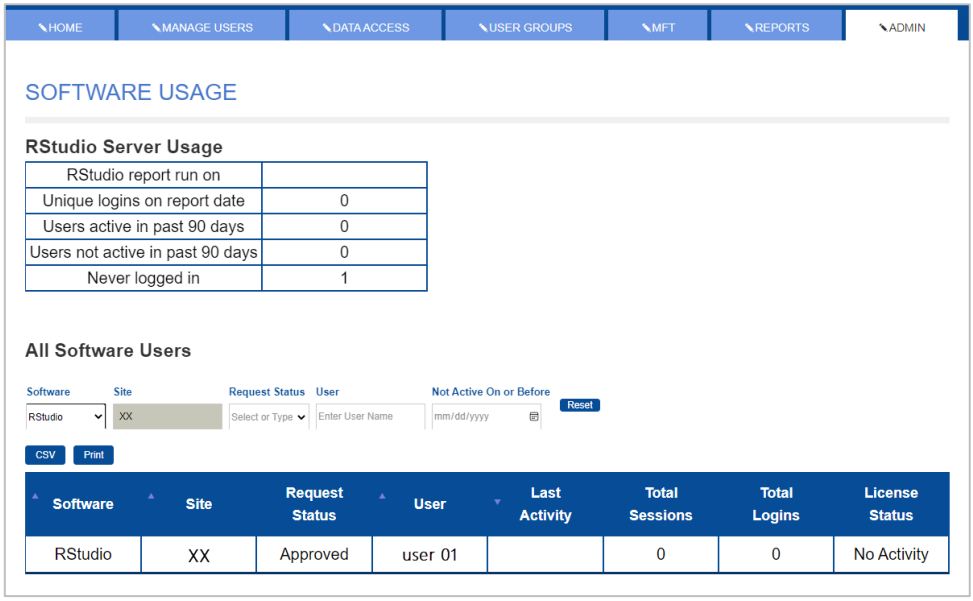


Figure 60. Admin Tab—Software Usage Available to Site

9.2 Operational Access View

There are additional functions available to operational access users (superusers.) These include access to the Notification Banner and the Software Request view, as well as the Software Usage view to which all site administrators have access (for their site).

9.2.1 Notification Banner

The Notification Banner allows informational, warning, and critical messages to be displayed on the login and Home pages. Messages can contain information about the status of the AMC application or any announcement pertinent to all BioSense Platform users. Messages are prefaced by a word: Informational, Warning, or Critical. These are color coded to indicate severity of the message.

The notification messages are stored in a database table. Each Notification Banner record consists of the message, the type of message, and start and end dates. For auditing purposes, the AMC user ID of the person creating or modifying the record and the timestamp when the record was created or modified is also recorded.

Since all users in all sites will see these notifications when they log on or view the AMC Home page, this should be used only for notices affecting the user community and not for notices that are site-specific.

9.2.2 Software Requests

The Software Requests section lists all users whose site administrator has requested a software license for their use. Superusers are also listed here when viewed by another superuser.

Currently, only Posit (RStudio) Workbench licenses and unfulfilled requests are tracked.

Filters are available to display licensees by Software (Posit [RStudio] only for now), Status (Approved, Removed, Added, Denied, Cancelled, or Pending), individual site or all sites (operational access use only), or specific User ID.

Filters are drop-down lists or dynamic text (string). Dynamic filters can locate records using partial strings.

9.2.3 Software Usage

Software usage includes information about License Detail, License Requests, License Server Usage, and a table of users. Currently, only RStudio/Posit information is displayed.

License Detail includes information about the number of licenses authorized and type (for example, per-seat), number of licenses assigned, and number of licenses still available to be assigned.

License Requests are displayed as a small table showing request status (Approved, Denied, Added, Removed, Cancelled, or Pending) and counts of requests with these statuses.

License Server Usage provides data about license usage from the application server. Information includes the date when the server report was run, count of unique logins on report date, users active in last 90 days, users not active in last 90 days, and users never logged in.

A table of users is at the bottom of Software Usage page. This table shows all users with software (currently Posit/RStudio only), Site, Request Status, User ID, Last Activity (timestamp), Total Sessions, Total Logins, and License Status.

10. Commonly Performed AMC Activities

These are common examples of activities that can be performed to check and view your data. This is not an exhaustive list of activities.

10.1 Site Administrators

1. Initially and every 90 days:
   Log in with provided credentials.
   a. Accept the Site Administrator Code of Conduct.
   b. Change your password.
2. View and edit user profile information.
3. Create users.
4. Create a user group.
5. View existing users.
6. Edit users.
7. Create *Public* or *Private* user groups. *Public* user groups may be used by any site administrator with access to AMC. Private user groups can only be used in the site where they were created.
8. Create Data Access Rules for individual users, *Public* user groups, and private user groups that the site administrator have created in their site. Site administrators may also grant access to users from other sites. When creating Data Access Rules, NSSP recommends that you confirm with the user that the Data Access Rule provides them with the desired data access in ESSENCE.
9. Request named user licenses for access to Posit (RStudio) Workbench. **Note:** If requesting a Workbench license for a user, make sure that you have granted the user access to DataMart.

10.2 Users

1. In the My Info section, initially and every 90 days, users should:
   a. Accept the Code of Conduct.
   b. Change their passwords.
2. View and edit their profile information.
3. In the NSSP Applications section, users can link directly to:
   a. ESSENCE
   b. Posit (RStudio) Workbench (License required)
   c. SAS Studio
   d. Data Quality Dashboards
   Note: Access depends on user profile setup and specific login privileges.
4. In NSSP Resources, users can link to:
   a. Service Desk
   b. NSSP Technical Resource Center
   c. NSSP Community of Practice Website
   d. Data Dictionary and Data Flow Requirements