BioSense Platform User Manual for the Access & Management Center

April 2021

Centers for Disease Control and Prevention
Center for Surveillance, Epidemiology, and Laboratory Services

Division of Health Informatics and Surveillance

Technical Assistance: support.syndromicsurveillance.org

The National Syndromic Surveillance Program (NSSP) promotes and advances development of the cloud-based BioSense Platform, a secure integrated electronic health information system that hosts standardized analytic tools and facilitates collaborative processes. The BioSense Platform is a product of CDC.

BioSense Platform User Manual for the Access & Management Center

April 2021

Produced by

Division of Health Informatics and Surveillance
Center for Surveillance, Epidemiology, and Laboratory Services
Centers for Disease Control and Prevention

Revision History

Date	Revisions
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 any of their site's users. They can control the user access to the ESSENCE National View and Chief Complaint Query Validation Tool. Access to the DataMart, RStudio Pro, 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 RStudio Pro 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 support.syndromicsurveillance.org.

This user manual will help you access and navigate the AMC's main features. The manual will be updated as functionality is added. **The username and password you use for the AMC are the same credentials you will use to log in to ESSENCE, RStudio Pro, and SAS Studio (if applicable).**

[This page intentionally left blank]

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.

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, RStudio Pro, 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**.

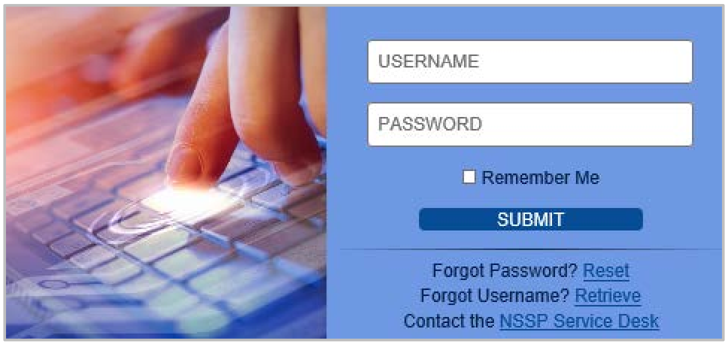
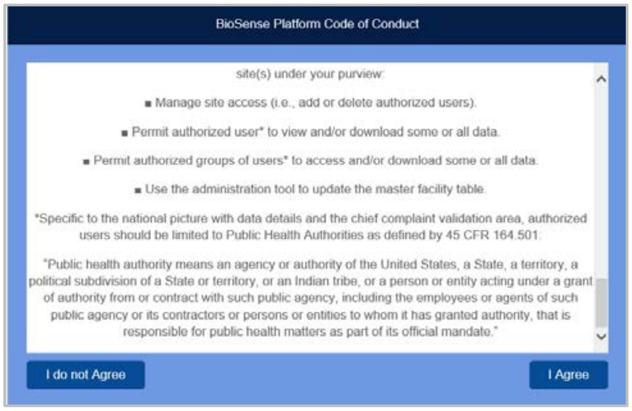


Figure 1. AMC Log-in Screen

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 (Figure 2). The Code of Conduct outlines proper practices and responsibilities (data-sharing etiquette) for the BioSense Platform user community.



site(s) under your purview:

- Manage site access (i.e., add or delete authorized users).
- Permit authorized user* to view and/or download some or all data.
- Permit authorized groups of users* to access and/or download some or all data.
- Use the administration tool to update the master facility table.

*Specific to the national picture with data details and the chief complaint validation area, authorized users should be limited to Public Health Authorities as defined by 45 CFR 164.501:

"Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate."

Figure 2. BioSense Platform Code of Conduct

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

- First time logging in.
- Every 90 days when password expires.
- User resets password.
- Changes are made to user's authorized access (e.g., if a user account becomes a site administrator account).

If the **I Agree** button is not active, we suggest that you change the browser zoom setting. Go to Settings and if, for example, you're using Chrome, look in the upper right corner of the screen and click on the three vertical dots. Then change the zoom setting from 100% to 90% (if 90% zoom does not work, 80% zoom usually works).

2.4 Activating Your Account

You must change your password the first time you log in to the AMC (Figure 3 below). You will not be able to access the AMC or other tools until you have accepted the BioSense Platform Code of Conduct and changed your password. **Note:** 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 minimum requirements listed below.

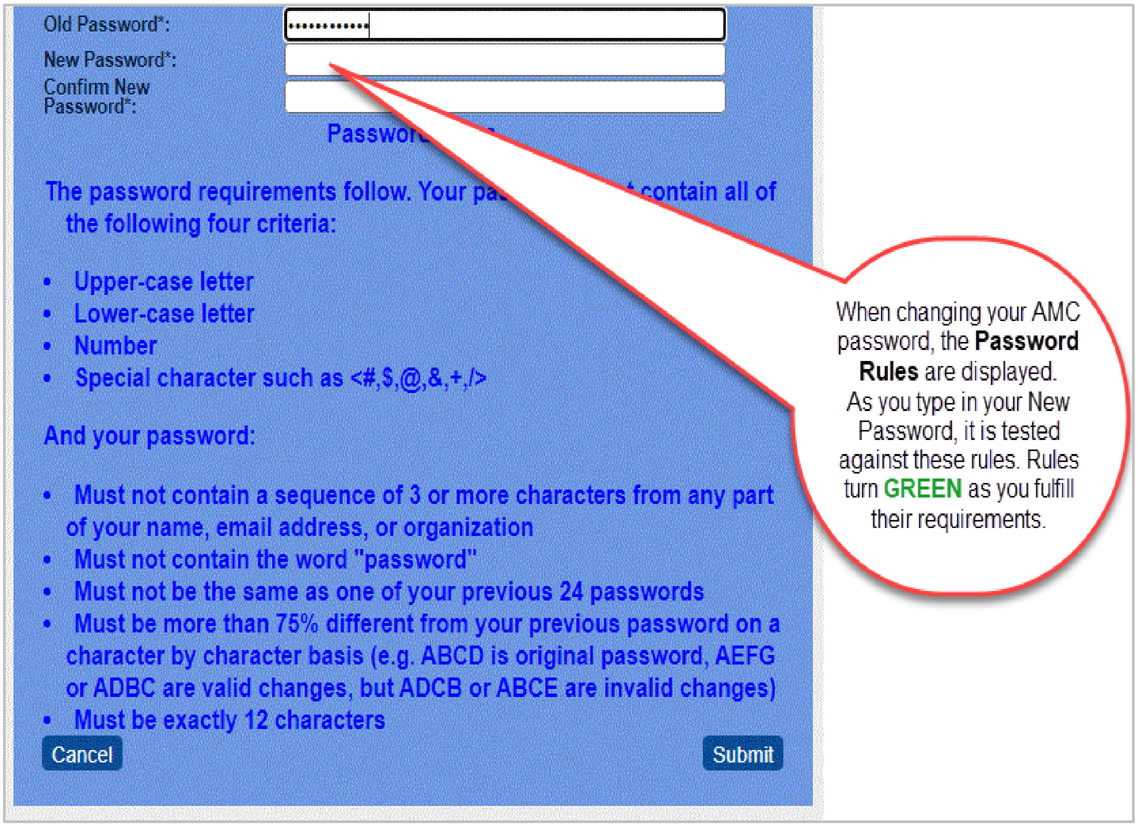
Password Requirements

- Passwords must meet 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
  - The word "password"
- Passwords must be more than 75% different from your previous password on a character-by-character basis (e.g., ABCD is original password, AEFG or ADBC are valid changes, but AECD or ABCE are invalid changes).
- Passwords must not match your previous 24 passwords.

- Since there are specific password requirements, we recommend using a random password generator for enhanced security. We suggest searching the internet for “Free Password Generator” for 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 user name and password combination is used for AMC, ESSENCE, RStudio Server Pro, and SAS Studio.** **Note:** This is accomplished with the Windows Active Directory (AD) functionality, so when you change your password, there may 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, RStudio Pro, 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):



Old Password*: ••••••••••••

New Password*:

Confirm New Password*:

Passwor

The password requirements follow. Your pa t contain all of the following four criteria:

- Upper-case letter
- Lower-case letter
- Number
- Special character such as <#,$,@,&,+,/>

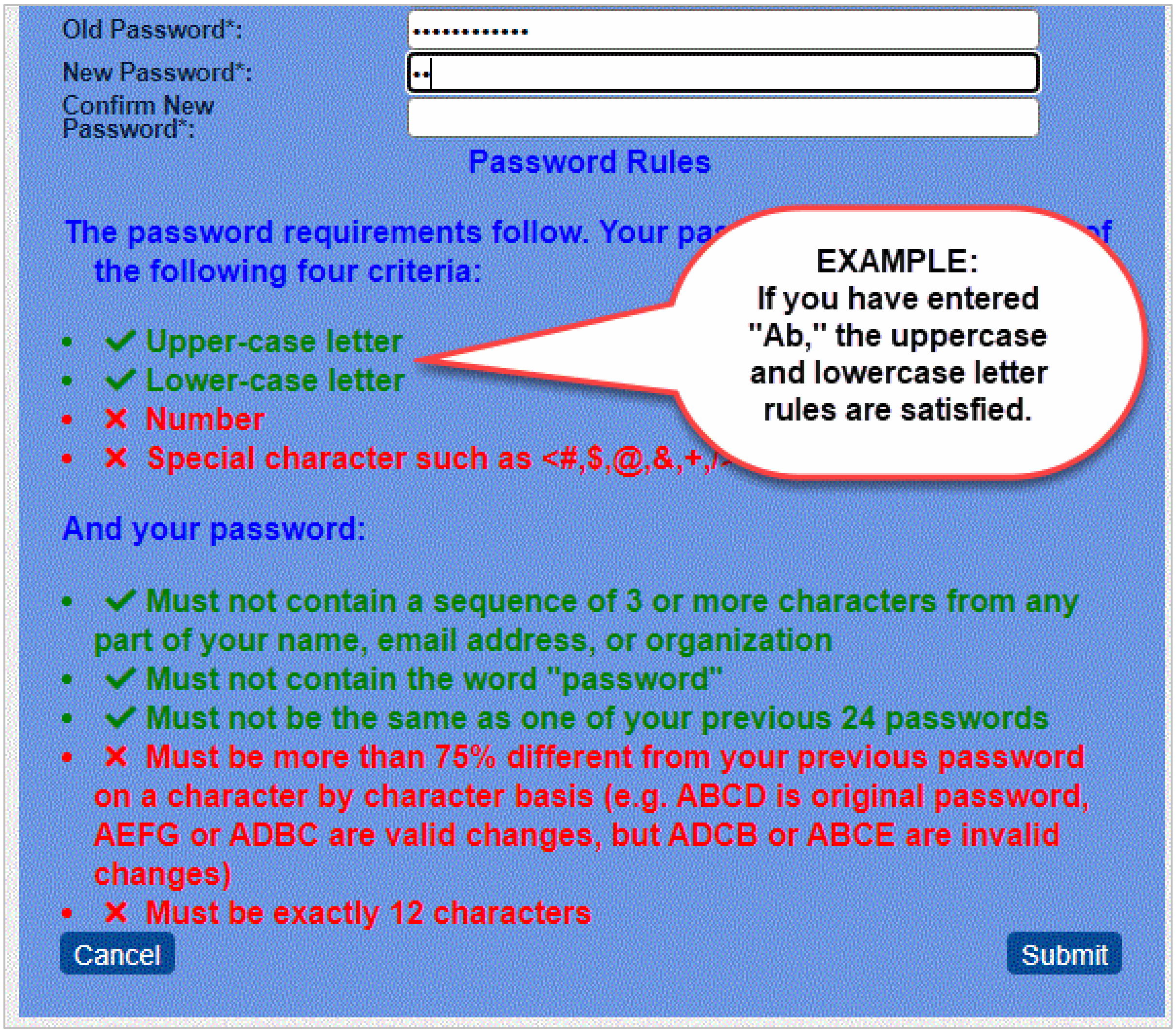
And your password:

- Must not contain a sequence of 3 or more characters from any part of your name, email address, or organization
- Must not contain the word "password"
- Must not be the same as one of your previous 24 passwords
- Must be more than 75% different from your previous password on a character by character basis (e.g. ABCD is original password, AEFG or ADBC are valid changes, but ADCB or ABCE are invalid changes)
- Must be exactly 12 characters

When changing your AMC password, the **Password Rules** are displayed. As you type in your New Password, it is tested against these rules. Rules turn **GREEN** as you fulfill their requirements.

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.



Old Password*: ••••••••••••

New Password*: ••

Confirm New Password*:

Password Rules

The password requirements follow. Your pa f
the following four criteria:

- ✓ Upper-case letter
- ✓ Lower-case letter
- ✗ Number
- ✗ Special character such as <#,$,@,&,+,/

And your password:

- ✓ Must not contain a sequence of 3 or more characters from any part of your name, email address, or organization
- ✓ Must not contain the word "password"
- ✓ Must not be the same as one of your previous 24 passwords
- ✗ Must be more than 75% different from your previous password on a character by character basis (e.g. ABCD is original password, AEFG or ADBC are valid changes, but ADCB or ABCE are invalid changes)
- ✗ Must be exactly 12 characters

EXAMPLE:
If you have entered "Ab," the uppercase and lowercase letter rules are satisfied.

Figure 4. Dynamic Password Rule Check

What if I forget my password?

Navigate to the AMC log-in page and click the "Forgot Password" link.

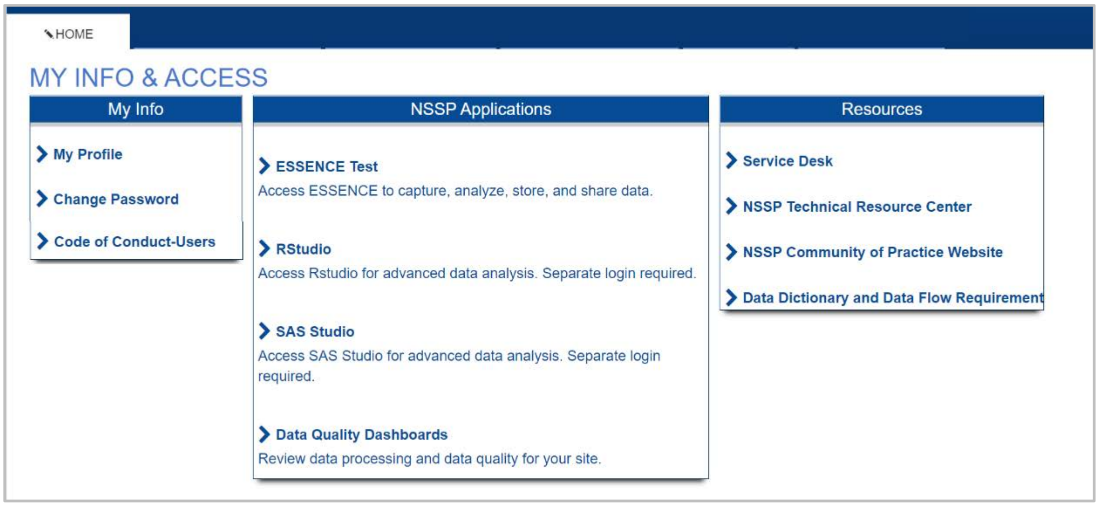
Provide the requested information to receive an email with a new one-time password.

- When you receive your new password, use it to log in to AMC.
- Once logged in, you will be taken directly to the Change Password screen and required to change your password before proceeding.
- Enter your one-time password as your "Old Password."

3. Home Page

3.1 User Home Page

The AMC home page (Figure 5) for users provides access to applications and links to useful resources:



HOME

MY INFO & ACCESS

My Info

- My Profile
- Change Password
- Code of Conduct-Users

NSSP Applications

- ESSENCE Test
  Access ESSENCE to capture, analyze, store, and share data.
- RStudio
  Access Rstudio for advanced data analysis. Separate login required.
- SAS Studio
  Access SAS Studio for advanced data analysis. Separate login required.
- Data Quality Dashboards
  Review data processing and data quality for your site.

Resources

- Service Desk
- NSSP Technical Resource Center
- NSSP Community of Practice Website
- Data Dictionary and Data Flow Requirement

Figure 5. AMC User Home Page

My Info

Users and site administrators can follow links to change passwords, update selected profile data, and view the Code of Conduct for using 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.
- ***RStudio Pro***—View MS SQL data and perform advanced data analysis.
- ***SAS Studio***—View MS SQL data and perform advanced data analysis.

Resources

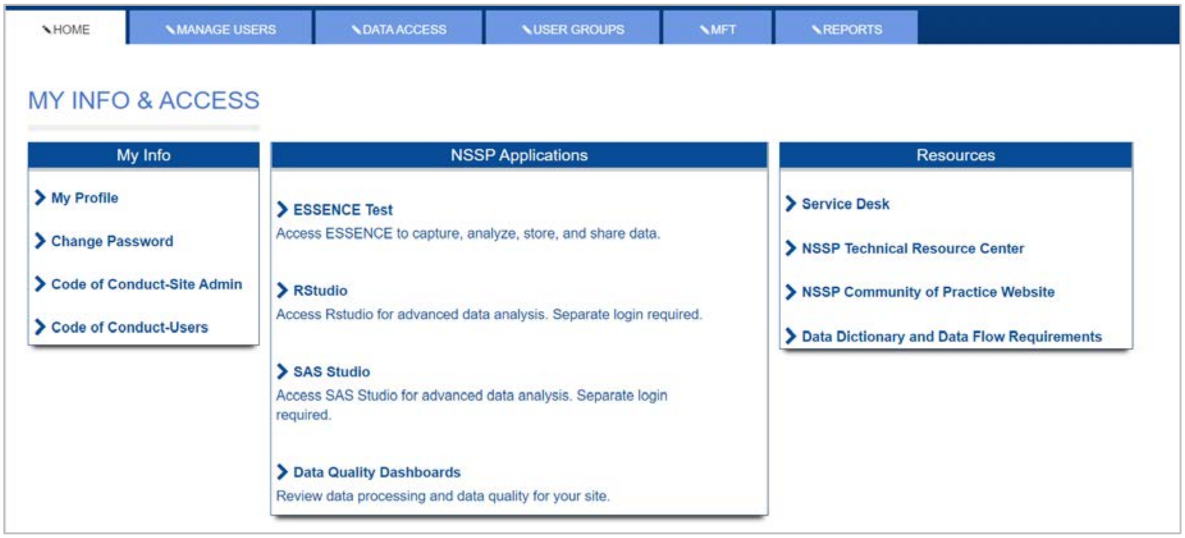
- ***NSSP Service Desk***—You will be asked to set up a password. Once you have a password, you may submit general or technical questions about NSSP. Your question will be routed to a specialist. Links to **Service Desk**
- ***NSSP Technical Resource Center***—This is a go-to place for NSSP publications (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. Links to **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.
  Links to **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. Links to **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***—Change password, update profile, and navigate to other BioSense Platform applications and resources.
- ***Manage Users***—Add, modify, or remove user accounts for your site.
- ***Data Access***—Add, modify, or remove data access permissions for ESSENCE accounts.
- ***User Groups***—Add, modify, or remove group members.
- ***Master Facility Table (MFT)***—Add, modify, or view facilities for your site.
- ***Reports***—View users who can access your data.



MY INFO & ACCESS

My Info

- My Profile
- Change Password
- Code of Conduct-Site Admin
- Code of Conduct-Users

NSSP Applications

- ESSENCE Test
  Access ESSENCE to capture, analyze, store, and share data.
- RStudio
  Access Rstudio for advanced data analysis. Separate login required.
- SAS Studio
  Access SAS Studio for advanced data analysis. Separate login required.
- Data Quality Dashboards
  Review data processing and data quality for your site.

Resources

- Service Desk
- NSSP Technical Resource Center
- NSSP Community of Practice Website
- Data Dictionary and Data Flow Requirements

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 the home page that allows them to see 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	NSSP	Dmckenziemeu01(Dan McKenzieMEU)	State	Data Quality (HHS Region)	N	
NSSP National View □ Aggregate Only	NSSP	Dmckenziemeu01(Dan McKenzieMEU)	State	National View Datasets	N	
NSSP National View □ Aggregate Only	NSSP	Dmckenziemeu01(Dan McKenzieMEU)	State	Region Syndrome Alert List	N	

Figure 7. Data You Can View in ESSENCE

4. Navigation

The AMC Home page is organized by tabs across the top. A list and description of each tab follows.

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.

My Info

You may update your profile, change your password, and view the Code of Conduct for users. As a site administrator, the functionality is similar, but you will be able to see the Code of Conduct for both users and site administrators.

NSSP Applications

Users and site administrators can gain quick access to tools and applications (ESSENCE, RStudio Pro, and SAS Studio).

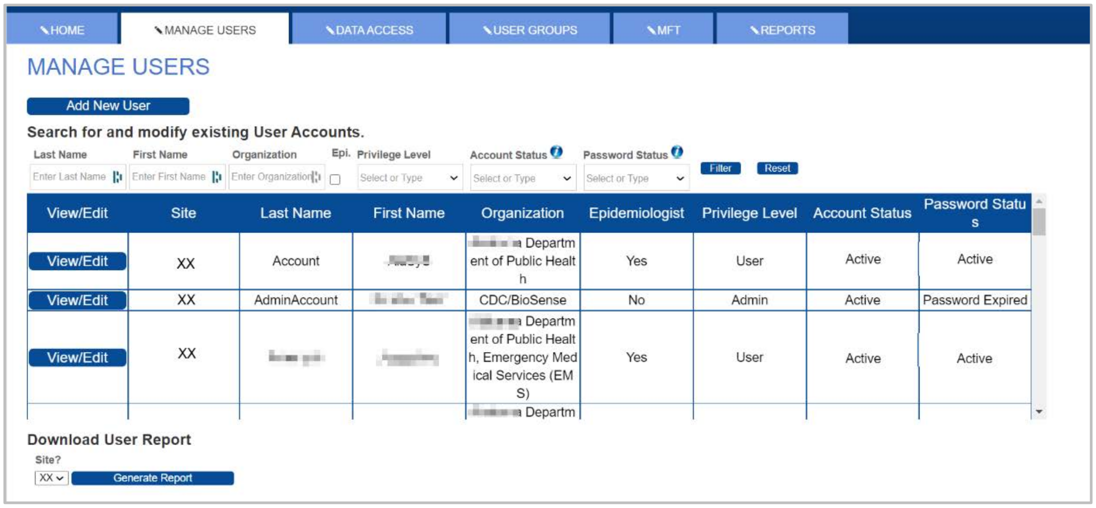
Resources

This section links to resources available to all users: Service Desk to request technical and general support; 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; and Data Dictionary and Data Flow Requirements.

4.2 Manage Users Tab (Site Administrators Only)

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

Site administrators are responsible for creating and managing the user accounts for their site.



MANAGE USERS

Add New User

Search for and modify existing User Accounts.

Last Name	First Name	Organization	Epi.	Privilege Level	Account Status	Password Status		
Enter Last Name	Enter First Name	Enter Organization	□	Select or Type	Select or Type	Select or Type	Filter	Reset

View/Edit	Site	Last Name	First Name	Organization	Epidemiologist	Privilege Level	Account Status	Password Status
View/Edit	XX	Account	[redacted]	[redacted] Department of Public Health	Yes	User	Active	Active
View/Edit	XX	AdminAccount	[redacted]	CDC/BioSense	No	Admin	Active	Password Expired
View/Edit	XX	[redacted]	[redacted]	[redacted] Department of Public Health, Emergency Medical Services (EMS)	Yes	User	Active	Active
				[redacted] Departm				

Download User Report

Site?

XX Generate Report

Figure 8. Manage Users Page

Create Users

To create a new user account, click **Add New User**. Provide the requested information and click **Save**. Once you successfully save a new user, an email containing log-in credentials will be sent to the 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.
- Users within your site must have unique email addresses.

Modify User Accounts

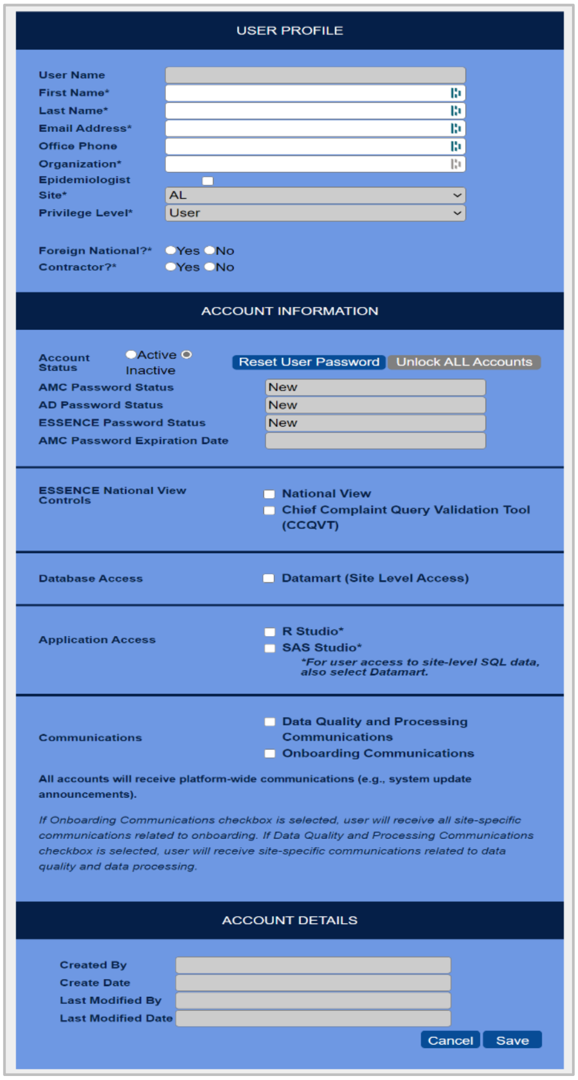
To review or modify a user account, select a row in the user table and click **View/Edit**. You will be able to see and update the user profile.

Removing (Deactivating) User Accounts

Due to CDC policy, user accounts cannot be deleted. If a user no longer requires access, select the account, click **View/Edit**, and change the Account Status radio button selection to "Inactive." If you deactivate a user in the AMC, that user will no longer be able to use the AMC or other BioSense Platform tools.

User Profile Page

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



USER PROFILE

User Name

First Name*

Last Name*

Email Address*

Office Phone

Organization*

Epidemiologist □

Site* AL

Privilege Level* User

Foreign National?* ○Yes ○No

Contractor?* ○Yes ○No

ACCOUNT INFORMATION

Account Status ○Active ○ Inactive

Reset User Password | Unlock ALL Accounts

AMC Password Status	New
AD Password Status	New
ESSENCE Password Status	New
AMC Password Expiration Date	

ESSENCE National View Controls
- □ National View
- □ Chief Complaint Query Validation Tool (CCQVT)

Database Access
- □ Datamart (Site Level Access)

Application Access
- □ R Studio*
- □ SAS Studio*

**For user access to site-level SQL data, also select Datamart.*

Communications
- □ Data Quality and Processing Communications
- □ Onboarding Communications

All accounts will receive platform-wide communications (e.g., system update announcements).

If Onboarding Communications checkbox is selected, user will receive all site-specific communications related to onboarding. If Data Quality and Processing Communications checkbox is selected, user will receive site-specific communications related to data quality and data processing.

ACCOUNT DETAILS

Created By

Create Date

Last Modified By

Last Modified Date

Figure 9. User Profile Page

User Profile

This section contains contact information and background.

- ***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.
- ***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.
- ***PIV Required***—This checkbox is checked if the user has a PIV card and requires a PIN code for logging in to both AMC and ESSENCE. Once checked, the U.S. Department of Health and Human Services (HHS) ID field and PIV Exception Status fields become visible. These fields are only editable by NSSP staff.
- ***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.
- ***PIV Exception Status***—"Active" indicates that PIV user may log in with a user name, password, and PIN code. To activate field, the site administrator must select the "Grant PIV Exception" button.
- ***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 permission. 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.

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 select 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. 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.
- ***AMC Password Status***—The status of the user's AMC account password.
- ***Active Directory Password Status***—The status of the user's Active Directory account password.
- ***ESSENCE Password Status***—The status of the user's ESSENCE account password.
- ***AMC Password Expiration Date***—The expiration date of the user's current password.

ESSENCE National View Controls—Site administrators may control which accounts can view the National View and Chief Complaint Query Validation data sources within ESSENCE. **By default, accounts do not have access to these data sources.**

- ***National View Aggregate Only***—Select this option to view the ESSENCE data sources "Patient Location (Limited Details by HSS 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).
- ***National View Aggregate and 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 view the ESSENCE data source "Chief Complaint Query Validation."

The National View data sources contain limited fields 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 National View data sources.

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 source.

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 MS SQL tables. Users may access SQL tables by using built-in functionality in RStudio Pro or SAS Studio. This option does 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 need to submit a Service Desk request.

Application Access—Site administrators may control which accounts have access to the RStudio Pro and SAS Studio applications. **By default, new user accounts do not have access to these tools.**

- ***RStudio Pro***—Select this option to allow users to access and visualize site-level SQL data via RStudio Pro. **You must also grant access to the DataMart.**
- ***SAS Studio***—Select this option to allow viewers to access and visualize site-level SQL data via SAS Studio. **You must also grant access to the DataMart.**

Site-specific Communications—Site administrators may control which user accounts receive site-specific communications. There are two categories of site-specific communications:

1. ***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
    - Daily BioSense Platform Site Processing Summary.
    - Quarterly Executive Data Quality Summary.
    - Monthly Data Quality Report emails (completeness, timeliness, validity).
    - Miscellaneous data quality issue information.
2. ***Onboarding Communications***—Select this option to allow a user to receive site-specific communications related to onboarding, including information about
    - Data validation and facility management emails (i.e., day-to-day onboarding operations).
    - Connectivity and technical assistance emails (e.g., feed setup).
    - Strategic onboarding initiatives emails (e.g., baseline cleanups).

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

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.
- ***Created 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.

[This page intentionally left blank]

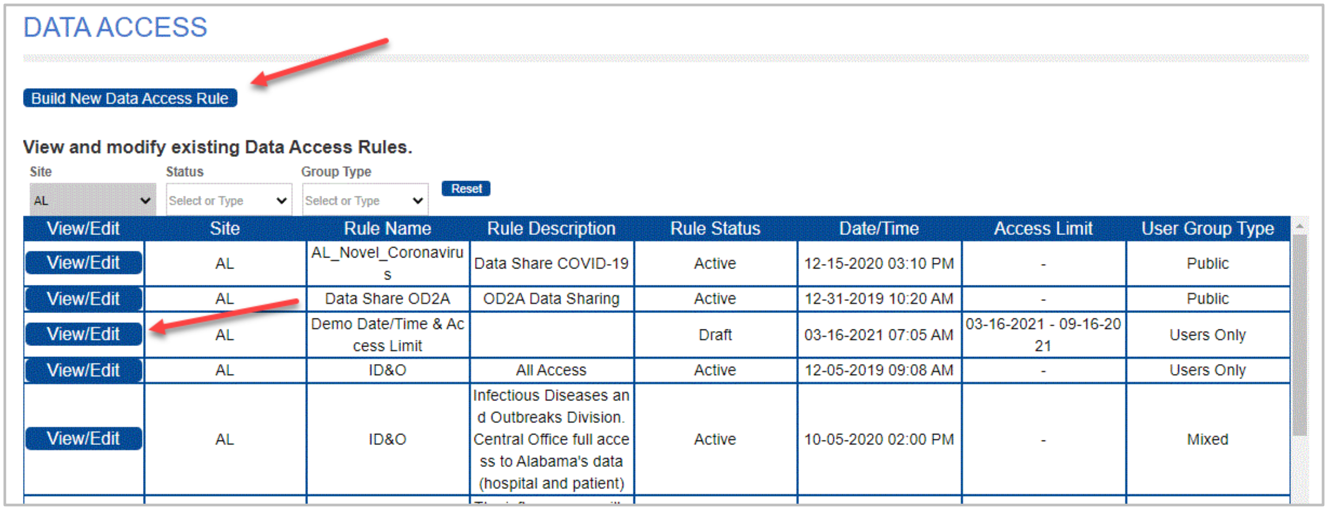
5. Data Access Rules

5.1 Create a Data Access Rule

Creating a data access rule for a user or site administrator in another site is the preferred method for sharing data between public health jurisdictions. Providing a user ID in your site for a user in another state can create maintenance issues over time.

Within AMC, the Data Access tab is only available to site administrators. As a site administrator, you may use this tab to create, review, and edit rules that control access to your site's data (Figure 10). Note the **red** arrows pointing to the **Build New Data Access Rule** and **View/Edit** buttons.

Data access rules can be applied to user accounts across NSSP–ESSENCE. You may create rules to grant data access to analysts and epidemiologists who work at your site, another site, or at CDC.



View and modify existing Data Access Rules.

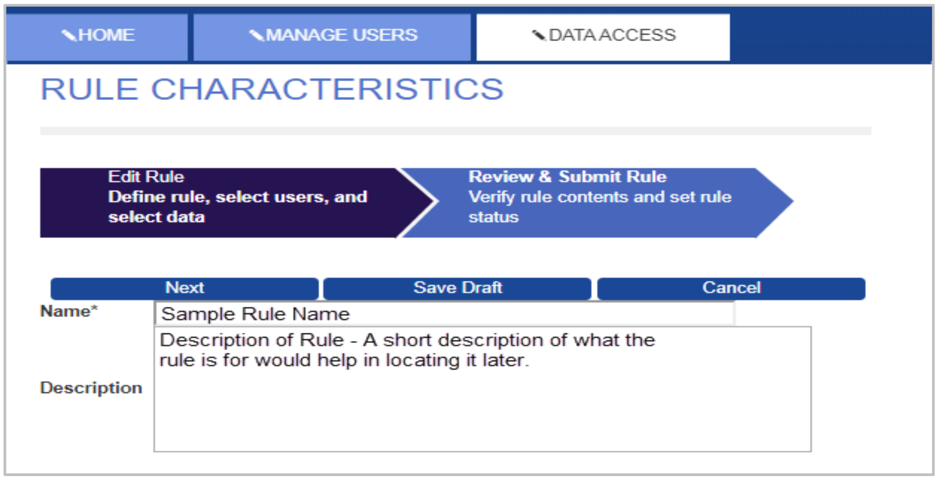
View/Edit	Site	Rule Name	Rule Description	Rule Status	Date/Time	Access Limit	User Group Type
View/Edit	AL	AL_Novel_Coronavirus	Data Share COVID-19	Active	12-15-2020 03:10 PM	-	Public
View/Edit	AL	Data Share OD2A	OD2A Data Sharing	Active	12-31-2019 10:20 AM	-	Public
View/Edit	AL	Demo Date/Time & Access Limit		Draft	03-16-2021 07:05 AM	03-16-2021 - 09-16-2021	Users Only
View/Edit	AL	ID&O	All Access	Active	12-05-2019 09:08 AM	-	Users Only
View/Edit	AL	ID&O	Infectious Diseases and Outbreaks Division. Central Office full access to Alabama's data (hospital and patient)	Active	10-05-2020 02:00 PM	-	Mixed

Figure 10. Build New Rule or View and Edit an Existing One

Note that the *Date/Time* column shows the date the rule was created or last modified, and the *Access Limit* column is populated if a *Data Access Time Limitation* was defined.

5.1.1 Rule Name and Description

Name your rule and enter a description (Figure 11). This will help you find your rule later.



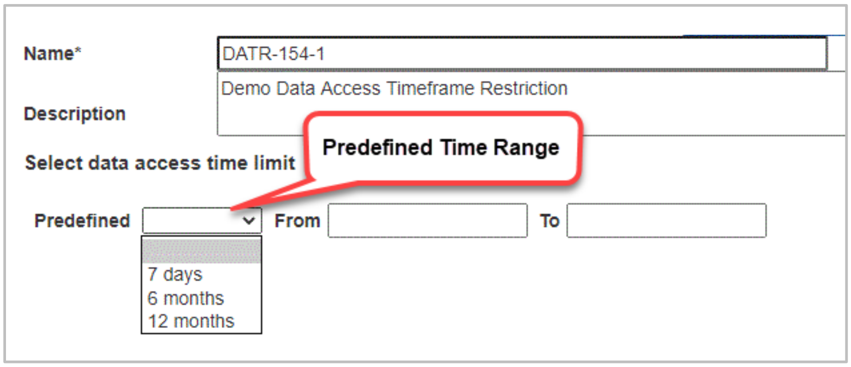
Name* Sample Rule Name

Description Description of Rule - A short description of what the rule is for would help in locating it later.

Figure 11. Name Your Rule and Add a Short Description

5.1.2 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 certain dates. For example, you may grant access to your site's data for a week, six months, or a year from the dropdown list (Figure 12), or you can enter a custom date range during which they will have access to the dataset defined by the data access rule.



Name* DATR-154-1

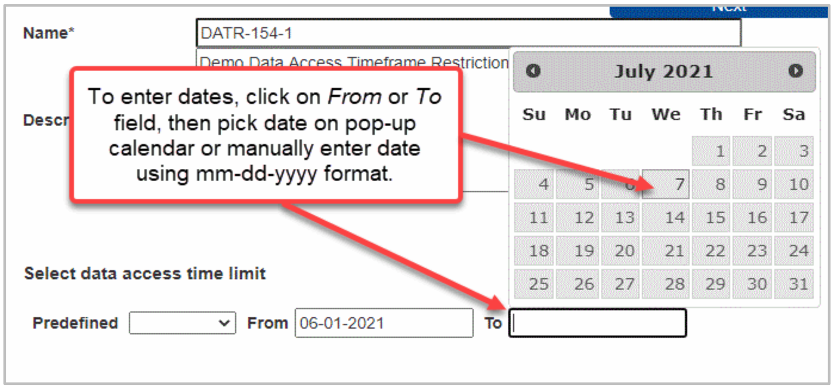
Description Demo Data Access Timeframe Restriction

Select data access time limit

Predefined From To

Figure 12. 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 13. Note that a pop-up calendar is displayed when you select each field and you may select dates directly from the calendar.



Name* DATR-154-1

Demo Data Access Timeframe Restriction

Descr

To enter dates, click on *From* or *To* field, then pick date on pop-up calendar or manually enter date using mm-dd-yyyy format.

July 2021

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Select data access time limit

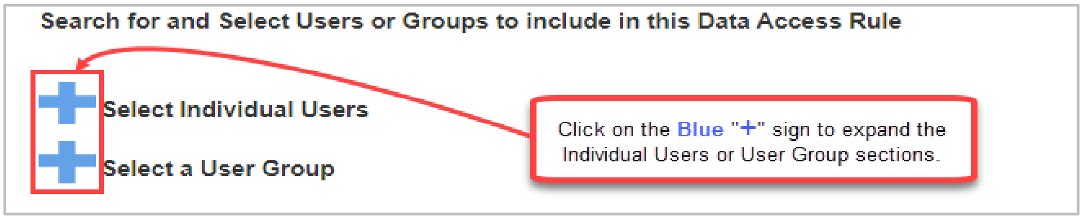
Predefined From 06-01-2021 To

Figure 13. Date-specified Time Range

When the current date falls outside the specified date range, the data access rule will automatically be suspended.

5.1.3 Select Users or 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 14).



Search for and Select Users or Groups to include in this Data Access Rule

Select Individual Users

Select a User Group

Click on the Blue "+" sign to expand the Individual Users or User Group sections.

Figure 14. Expand Users or Groups

Data should be shared with *purpose.* Carefully consider who needs data access and should be included in the Data Access Rule. Keep in mind that any user selected here (Figure 15) will receive access to the data source(s) you specify in the next step. You may designate individual users and groups of users.

Note that 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 their subsections are each sorted alphabetically.

You may use the fields directly below “Select Individual Users” and “Select a User Group” headings to filter the “Available” lists. When searching for the Last Name or First Name of a user, results can have characters that you enter appearing in any contiguous location within the name (e.g., “**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 15). **Note:** Site-defined user groups must be created before adding to a data access rule.

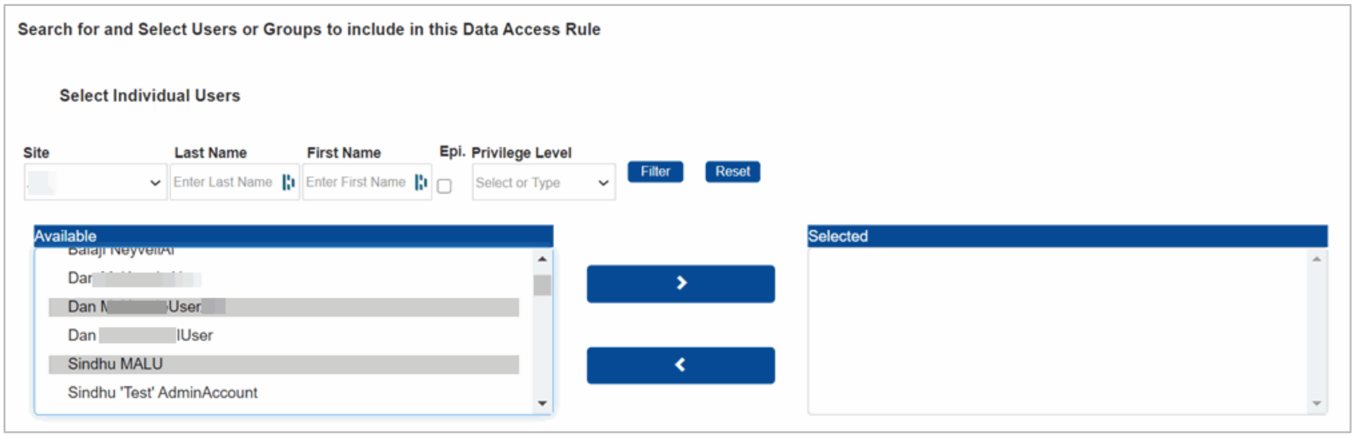
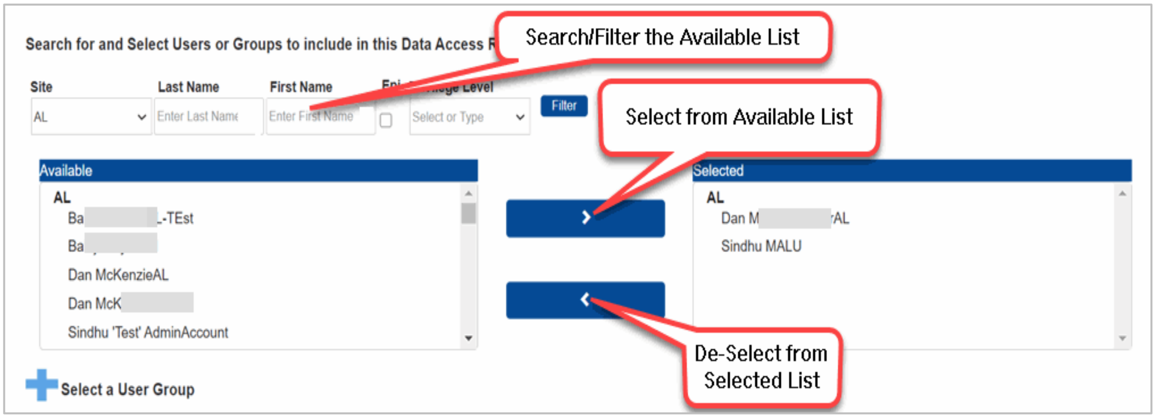


Figure 15. Data Access Page (Rule Characteristics—Select Users and Groups)

After highlighting users and groups in the "Available" boxes, click the "right" Arrow button (**>**) shown between the pick boxes to move them to the "Selected" boxes (Figure 16). You may select more than one individual or group to add (>) from the "Available" pick box or to move them back (<) from "Selected" to "Available."

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



Search/Filter the Available List

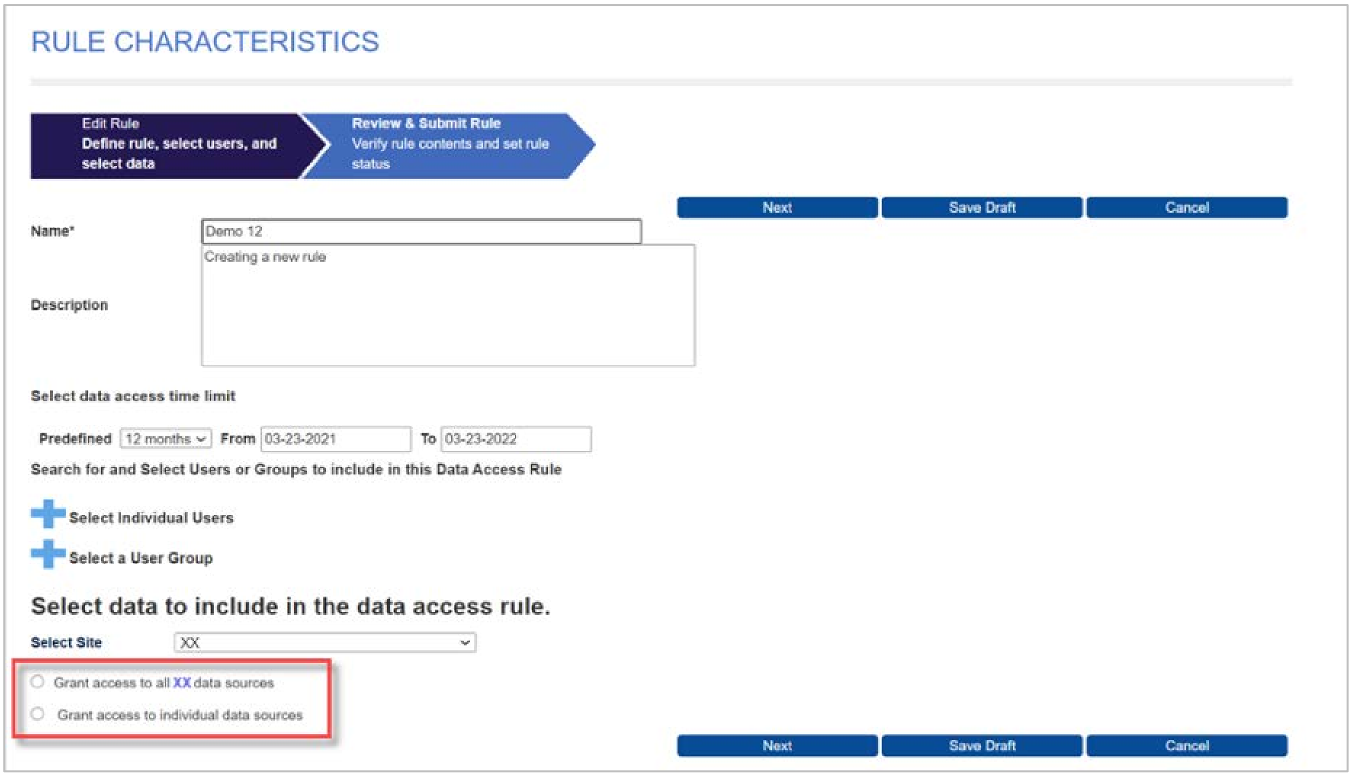
Select from Available List

De-Select from Selected List

Figure 16. Selecting Users from "Available" Pick Box

5.1.4 Selecting Data Sources

Next, select the data source(s) you want included in the Data Access Rule (Figure 17). 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. You may also restrict users from accessing your site's data by facility or by state and county.


Edit Rule
Define rule, select users, and select data
Review & Submit Rule
Verify rule contents and set rule status
Next
Save Draft
Cancel

RULE CHARACTERISTICS

Name* Demo 12

Description Creating a new rule

Select data access time limit

Predefined 12 months From 03-23-2021 To 03-23-2022

Search for and Select Users or Groups to include in this Data Access Rule

Select Individual Users

Select a User Group

Select data to include in the data access rule.

Select Site XX

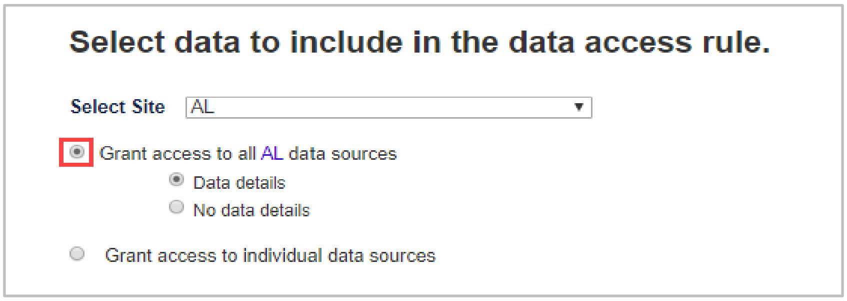
○ Grant access to all XX data sources

○ Grant access to individual data sources

Figure 17. Data Access Page—(Select Data)

5.1.5 Access to All Data Sources

Site administrators have the option to grant access to all data sources (Figure 18) 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.



Select data to include in the data access rule.

Select Site AL

● Grant access to all AL data sources

● Data details

○ No data details

○ Grant access to individual data sources

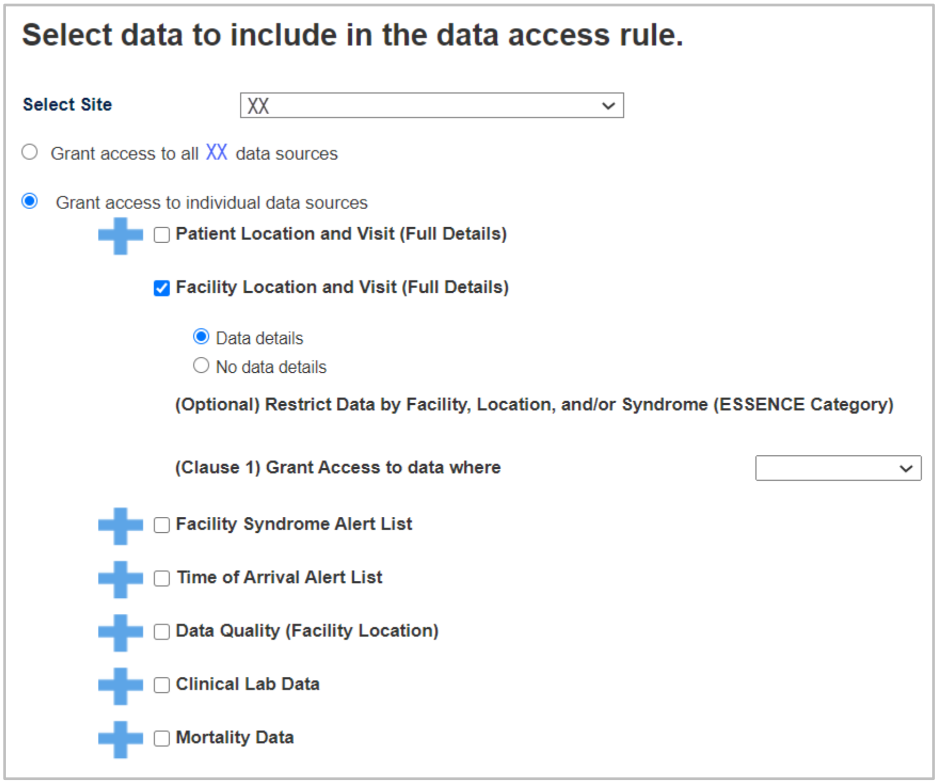
Figure 18. Data Access Page (Grant Access to All Data Sources)

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

By selecting "No data details," affected users can only view high-level data in ESSENCE via charts, graphs, and maps. However, the user will not have access to line-level data. For example, when running a query against a data source where "No data details" was selected, a user can view the time series graph but cannot click the graph to view patient information.

5.1.6 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 checkbox next to the data source (Figure 19). This will expand the data source and let you select the data layer and apply optional data restrictions.



Select data to include in the data access rule.

Select Site: XX

○ Grant access to all XX data sources

● Grant access to individual data sources

- □ Patient Location and Visit (Full Details)
- ☑ Facility Location and Visit (Full Details)
  - ● Data details
  - ○ No data details
  - (Optional) Restrict Data by Facility, Location, and/or Syndrome (ESSENCE Category)
  - (Clause 1) Grant Access to data where
- □ Facility Syndrome Alert List
- □ Time of Arrival Alert List
- □ Data Quality (Facility Location)
- □ Clinical Lab Data
- □ Mortality Data

Figure 19. Data Access Page (Grant Access to Individual Data Sources)

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 (e.g., 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 (e.g., 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.
- ***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.

5.1.7 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 is a list of sources and the dates in ESSENCE used to specify the records to be included within the timeframe.

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

The *timeframe* can be open or closed. For example, you may manually enter the start date (Timeframe-From), but no end date to allow ESSENCE to select all records from that date forward or only enter an end date (Timeframe-To) without a start date to constrain the selection to all records up to that date.

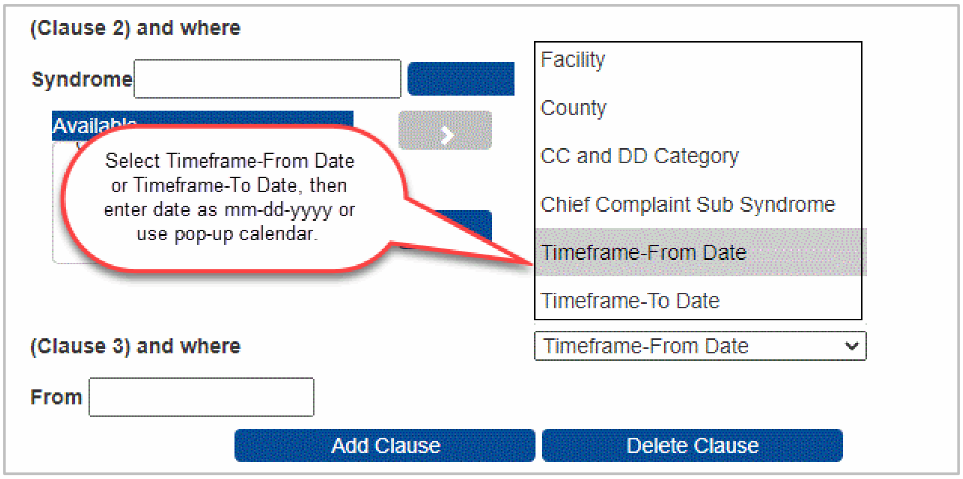
To select a closed timeframe option, enter two clauses, Timeframe-From and Timeframe-To dates. This is used to initiate a search for all records with a date within that range. That is, ESSENCE will only show records with dates within that timeframe. The dates will be selected using the date type noted 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 20) 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.

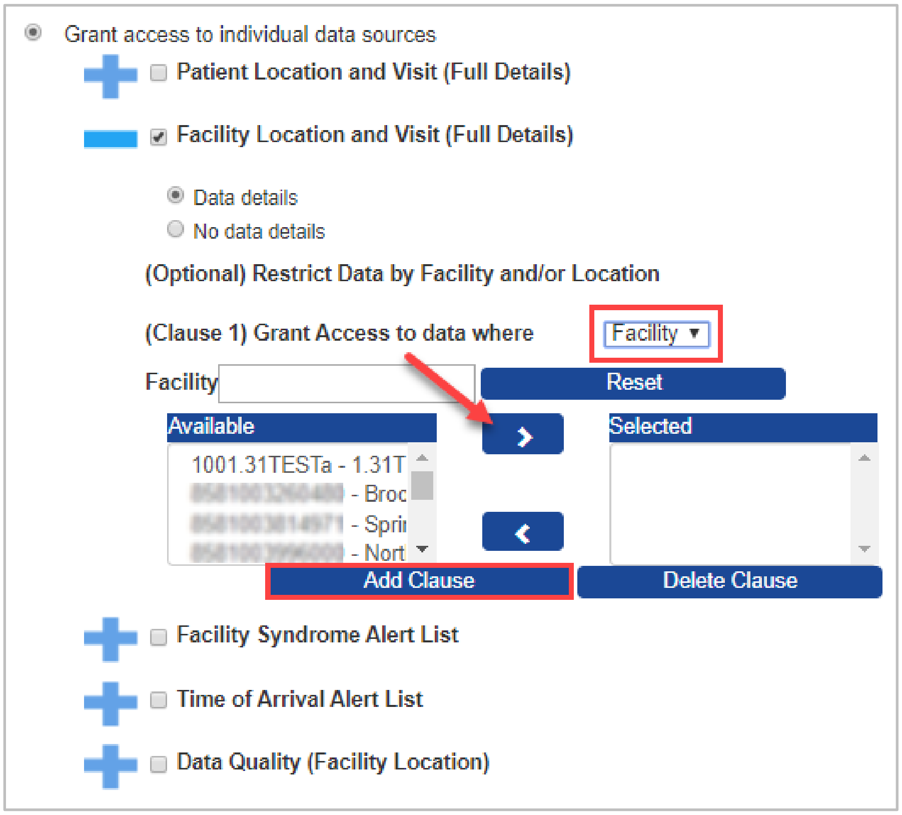


Select Timeframe-From Date or Timeframe-To Date, then enter date as mm-dd-yyyy or use pop-up calendar.

Figure 20. Setting up a Data Access Timeframe Restriction for a Data Source

5.1.8 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 or county) (Figure 21). To apply these optional restrictions, select Facility or Location (state or 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 selected data on the "Review & Submit Rule" page (Section 5.2).



● Grant access to individual data sources

□ Patient Location and Visit (Full Details)

☑ Facility Location and Visit (Full Details)

● Data details

○ No data details

(Optional) Restrict Data by Facility and/or Location

(Clause 1) Grant Access to data where Facility ▾

Facility

Available

1001.31TESTa - 1.31T
[redacted] - Broc
[redacted] - Sprii
[redacted] - Nort

Selected

□ Facility Syndrome Alert List

□ Time of Arrival Alert List

□ Data Quality (Facility Location)

Figure 21. Data Access Page (Grant Access to Individual Data Sources)

5.1.9 Access to Multiple Data Sources

To add additional data sources (Figure 22), 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.

How many clauses may I add, and how do I remove a clause?

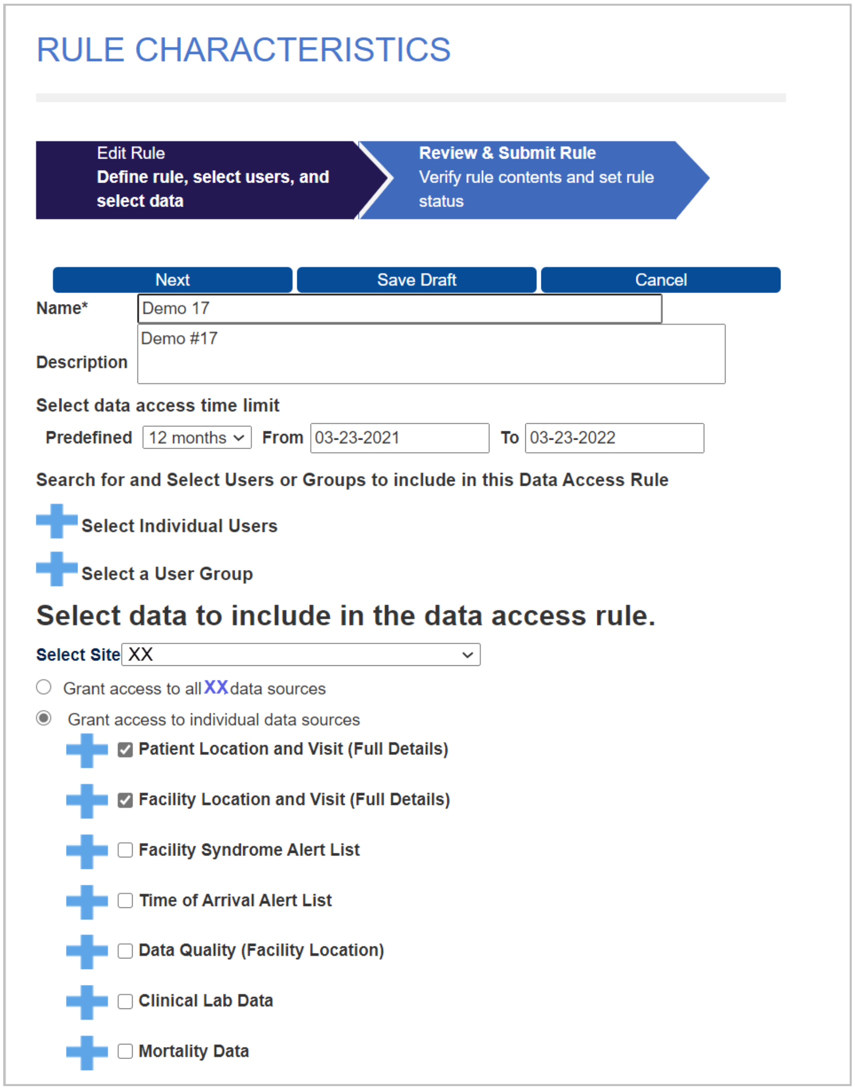
For Patient Location and Visit (Full Details) and Facility Location and Visit (Full Details) data sources, site administrators may add up to six (6) clauses when Data details is selected—State, County, Facility, CC and DD Category, Syndrome, Chief Complaint Sub Category, Timeframe-From Date, and Timeframe-To Date.

For No data details and other data sources, up to five (5) clauses may be specified—one for State, County, Facility, Timeframe-From Date, and Timeframe-To Date.

Note: When you select multiple clauses in a rule, all clauses must be satisfied for a record to be chosen, so selecting County and Syndrome, for example, creates an AND restriction,

e.g., WHERE County=my_cty **AND** Syndrome=ILI

To remove a clause, click the **Remove Clause** button under that Data Restriction’s pick box.



RULE CHARACTERISTICS

Edit Rule
Define rule, select users, and select data
Review & Submit Rule
Verify rule contents and set rule status
Next
Save Draft
Cancel

Name* Demo 17

Description Demo #17

Select data access time limit

Predefined 12 months From 03-23-2021 To 03-23-2022

Search for and Select Users or Groups to include in this Data Access Rule

Select Individual Users

Select a User Group

Select data to include in the data access rule.

Select Site XX

○ Grant access to all XX data sources

● Grant access to individual data sources

- ☑ Patient Location and Visit (Full Details)
- ☑ Facility Location and Visit (Full Details)
- □ Facility Syndrome Alert List
- □ Time of Arrival Alert List
- □ Data Quality (Facility Location)
- □ Clinical Lab Data
- □ Mortality Data

Figure 22. 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.

5.1.10 Selecting Syndromic Restrictions

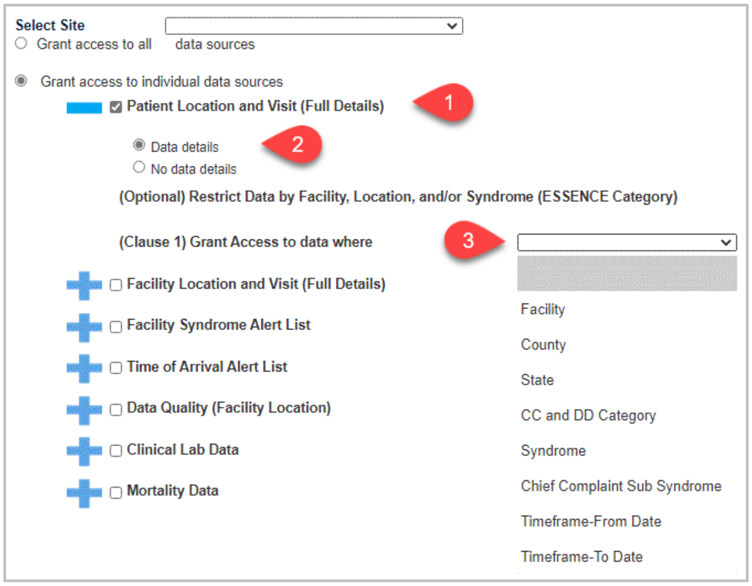
Syndromic restrictions can be applied to users or user groups by choosing “Grant access to individual data sources” and either Patient Location and Visit (Full Details) or Facility Location and Visit (Full Details) with “Data details.” These restrictions are applied by selecting CC and DD Category, Syndrome, and Chief Complaint Sub Syndrome for the WHERE clauses.

Both “Data details” and “No data details” selections continue to provide restriction by State, County, and Facility, but CC and DD Category, Syndrome, and Chief Complaint Sub Syndrome are only available if “Data Details” is selected.

As seen in Figure 23, when you choose **(1)** “Grant access to individual data sources” and select **(2)** “Data details,” then **(3)** click the **Grant Access to data where** dropdown list, the additional syndromic selections are displayed:

- State
- County
- Facility
- CC and DD Category
- Syndrome
- Chief Complaint Sub Syndrome
- Timeframe-From Date
- Timeframe-To Date

This allows up to eight (8) restricting clauses to be specified.



Select Site

○ Grant access to all data sources

● Grant access to individual data sources

☑ Patient Location and Visit (Full Details)

● Data details

○ No data details

(Optional) Restrict Data by Facility, Location, and/or Syndrome (ESSENCE Category)

(Clause 1) Grant Access to data where

☐ Facility Location and Visit (Full Details)

☐ Facility Syndrome Alert List

☐ Time of Arrival Alert List

☐ Data Quality (Facility Location)

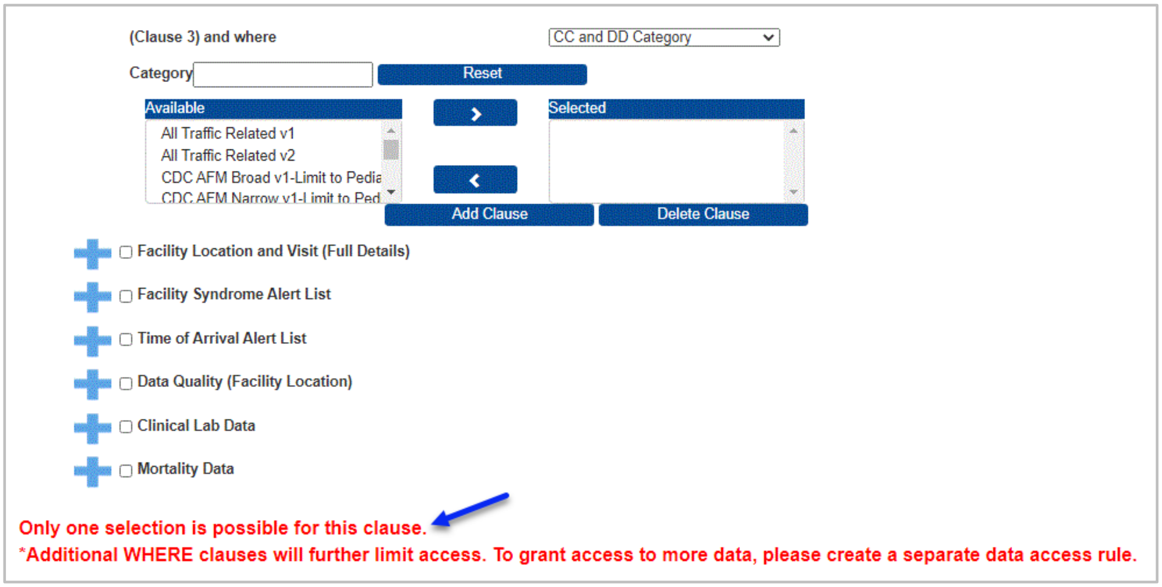
☐ Clinical Lab Data

☐ Mortality Data

Figure 23. Data Access—Building the WHERE Clause

State, Facility, and County values may include multiple selections. To include multiple selections, 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 24).



(Clause 3) and where: CC and DD Category

Category:

Available:
- All Traffic Related v1
- All Traffic Related v2
- CDC AFM Broad v1-Limit to Pedia
- CDC AFM Narrow v1-Limit to Ped

Selected:

- □ Facility Location and Visit (Full Details)
- □ Facility Syndrome Alert List
- □ Time of Arrival Alert List
- □ Data Quality (Facility Location)
- □ Clinical Lab Data
- □ Mortality Data

Only one selection is possible for this clause.

***Additional WHERE clauses will further limit access. To grant access to more data, please create a separate data access rule.**

Figure 24. Data Access Rule—Only One Selection Message

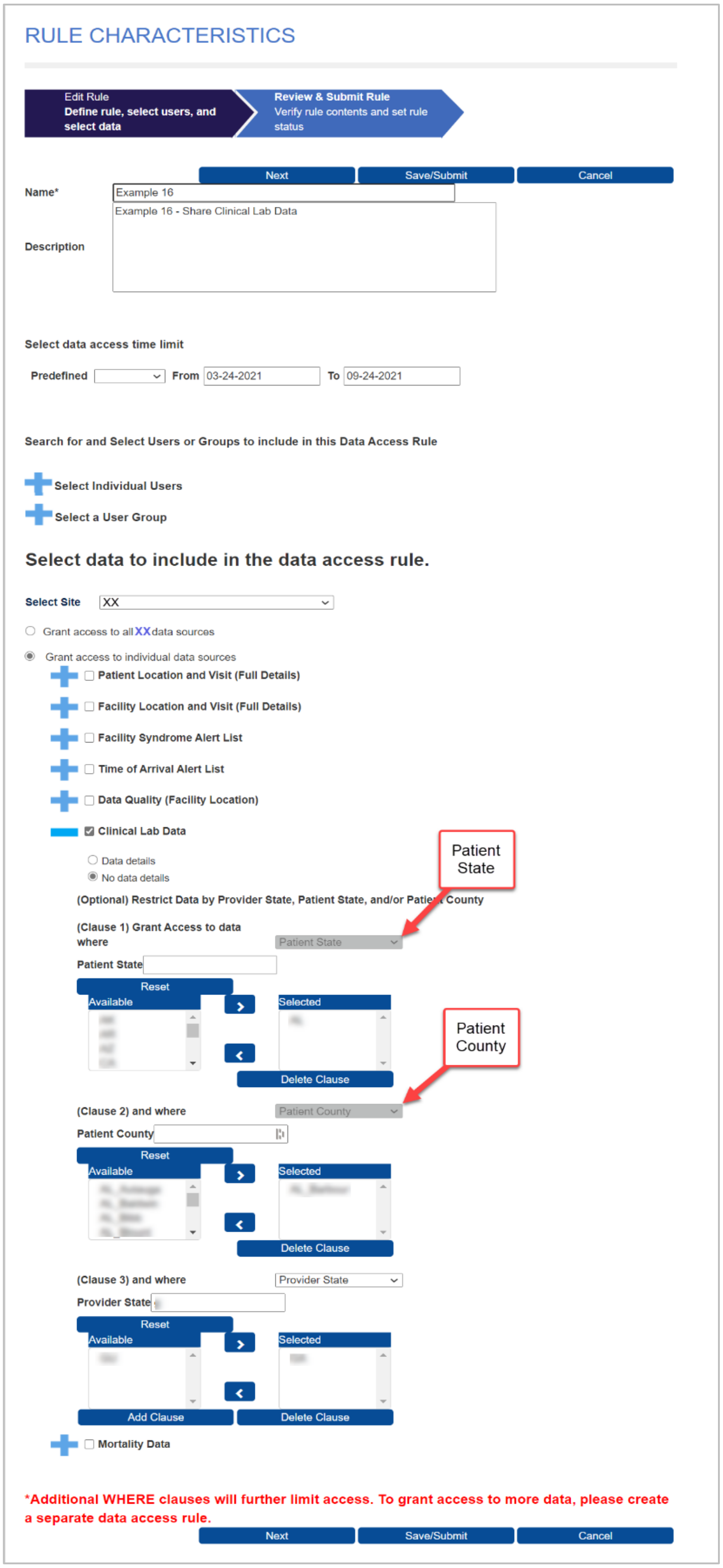
5.1.11 Selecting Clinical Laboratory Data

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 (super administrators). These administrators are now able to:

- Create data access rules in AMC for Clinical Laboratory Data that include WHERE clauses for Patient State, Patient County, and Provider State.
- Edit an existing rule to:
  - Add states and counties to be included in a data access rule.
  - Remove clauses (e.g., 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 25 provides an example of creating a new Clinical Laboratory Data rule.



RULE CHARACTERISTICS

Edit Rule
Define rule, select users, and select data

Review & Submit Rule
Verify rule contents and set rule status

Next | Save/Submit | Cancel

Name* Example 16

Description Example 16 - Share Clinical Lab Data

Select data access time limit

Predefined From 03-24-2021 To 09-24-2021

Search for and Select Users or Groups to include in this Data Access Rule

Select Individual Users

Select a User Group

Select data to include in the data access rule.

Select Site XX

○ Grant access to all XX data sources

● Grant access to individual data sources

- □ Patient Location and Visit (Full Details)
- □ Facility Location and Visit (Full Details)
- □ Facility Syndrome Alert List
- □ Time of Arrival Alert List
- □ Data Quality (Facility Location)
- ☑ Clinical Lab Data

○ Data details
● No data details

(Optional) Restrict Data by Provider State, Patient State, and/or Patient County

(Clause 1) Grant Access to data where Patient State

Patient State

Reset

Available: [redacted]

Selected: [redacted]

Delete Clause

(Clause 2) and where Patient County

Patient County

Reset

Available: [redacted]

Selected: [redacted]

Delete Clause

(Clause 3) and where Provider State

Provider State

Reset

Available: [redacted]

Selected: [redacted]

Add Clause | Delete Clause

- □ Mortality Data

*Additional WHERE clauses will further limit access. To grant access to more data, please create a separate data access rule.

Next | Save/Submit | Cancel

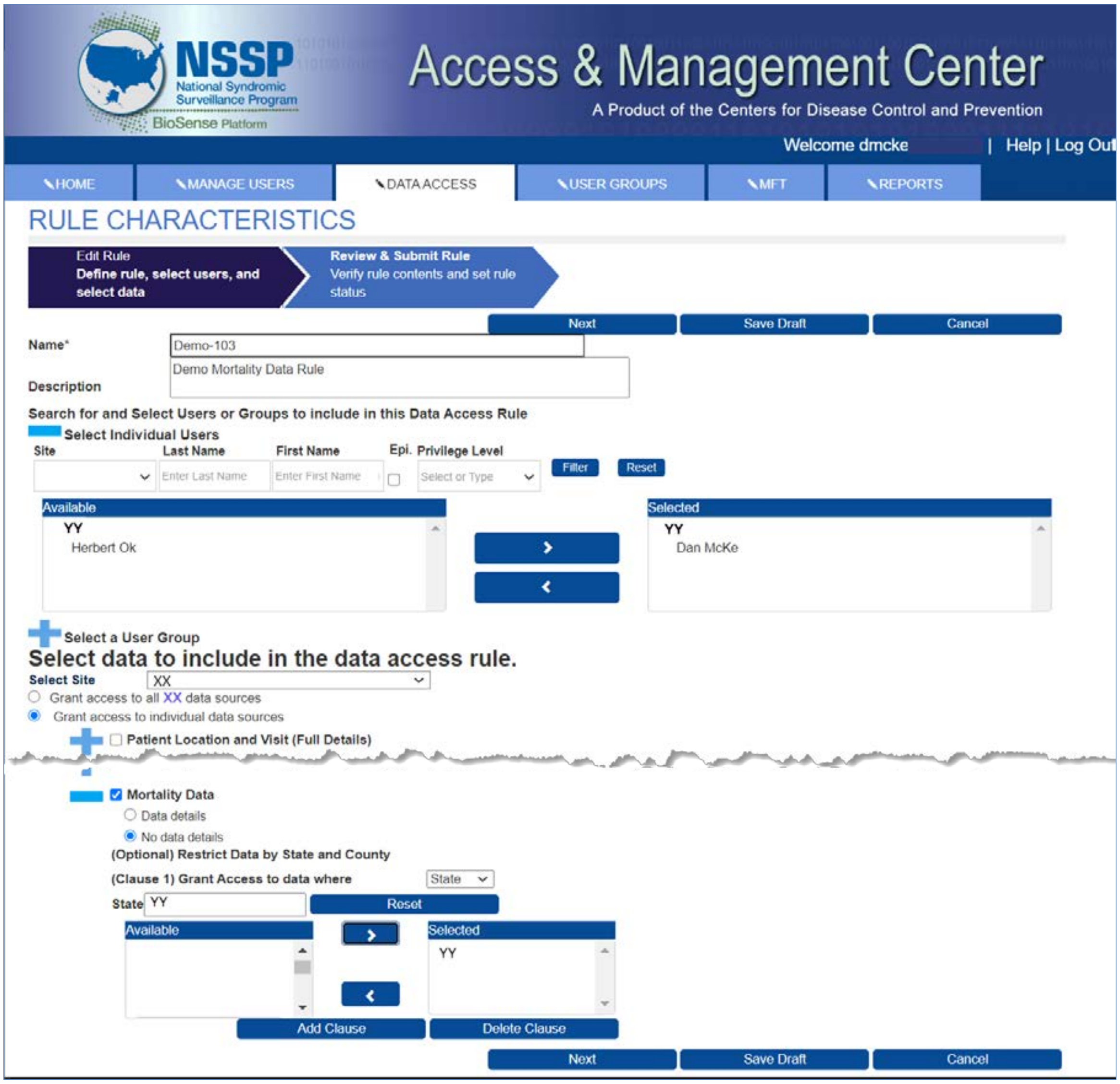
Figure 25. Data Access Build New Rule—Share Clinical Lab Data for Patients from a Neighboring State

5.1.12 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 now grant access to state mortality data. Access is limited by state and county. Figure 26 below illustrates the clauses used to provide access to select users in a bordering state with access to mortality data recorded in counties bordering the two states.

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


NSSP
National Syndromic Surveillance Program
BioSense Platform
Access & Management Center
A Product of the Centers for Disease Control and Prevention
Welcome dmcke
| Help | Log Out
HOME
MANAGE USERS
DATA ACCESS
USER GROUPS
MFT
REPORTS
Edit Rule
Define rule, select users, and select data
Review & Submit Rule
Verify rule contents and set rule status
Next
Save Draft
Cancel
Filter
Reset
Add Clause
Delete Clause

RULE CHARACTERISTICS

Name* Demo-103

Description Demo Mortality Data Rule

Search for and Select Users or Groups to include in this Data Access Rule

Select Individual Users

Site | Last Name: Enter Last Name | First Name: Enter First Name | Epi. ☐ | Privilege Level: Select or Type

Available: YY – Herbert Ok

Selected: YY – Dan McKe

Select a User Group

Select data to include in the data access rule.

Select Site: XX

○ Grant access to all XX data sources

● Grant access to individual data sources

☐ Patient Location and Visit (Full Details)

☑ Mortality Data

○ Data details

● No data details

(Optional) Restrict Data by State and County

(Clause 1) Grant Access to data where: State

State: YY

Available:

Selected: YY

Figure 26. Add New Data Access Rule for Mortality Data

5.2 Review and Submit the Rule

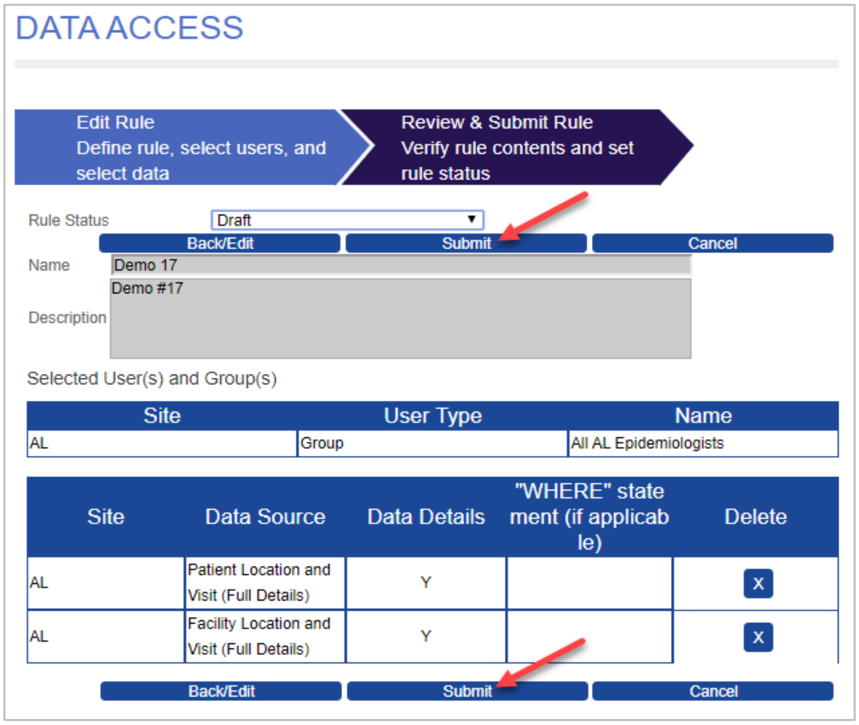
Once you name your rule and select users and data, you're ready to submit and implement your Data Access Rule. First, confirm that your selections are as expected. If you need to make changes, use the **Back/Edit** button to return to the Edit Rule page. Next, select the appropriate status for your rule (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.
- **Active:** This indicates that the rule has been submitted to ESSENCE and is being used to filter ESSENCE data based on 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, it 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 and will remain in the AMC. It can be activated from either the *Draft* or *Suspend* state.


DATA ACCESS
Edit Rule
Define rule, select users, and select data
Review & Submit Rule
Verify rule contents and set rule status
Back/Edit
Submit
Cancel

Rule Status: Draft

Name: Demo 17

Description: Demo #17

Selected User(s) and Group(s)

Site	User Type	Name
AL	Group	All AL Epidemiologists

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

Figure 27. Data Access Page (Review and Submit Rule)

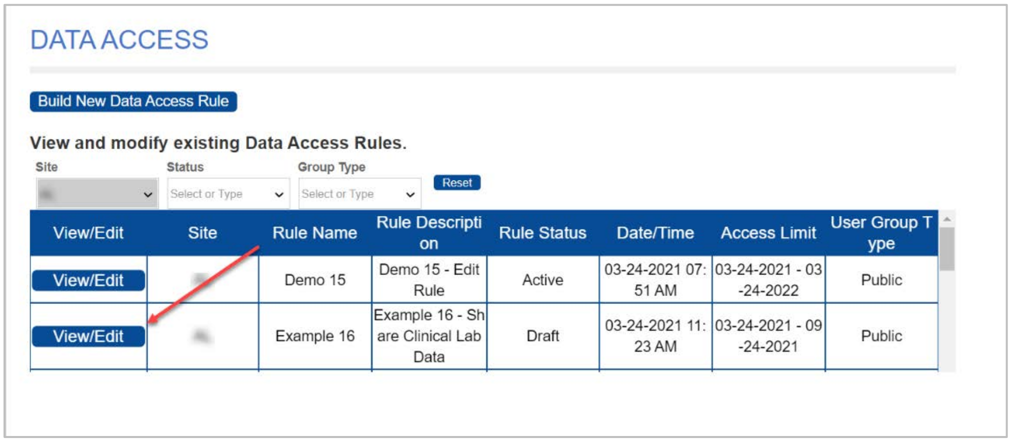
When you're done, click the **Submit** button (Figure 27). You'll be returned to the Data Access tab.

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 are not active in ESSENCE.

6. Edit a Rule

6.1 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 28).



DATA ACCESS

View and modify existing Data Access Rules.

Site: [redacted]

Status: Select or Type

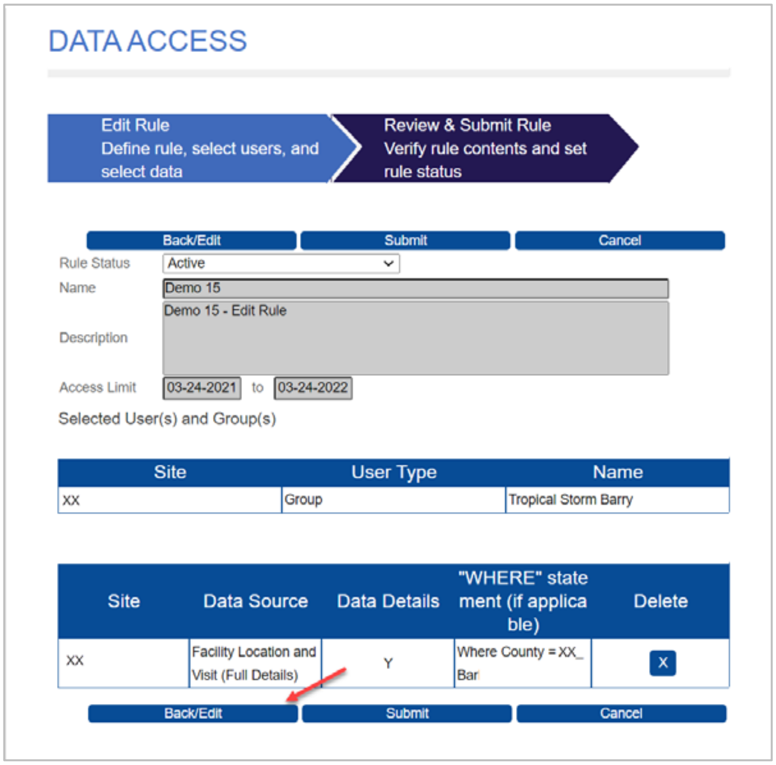
Group Type: Select or Type

View/Edit	Site	Rule Name	Rule Description	Rule Status	Date/Time	Access Limit	User Group Type
View/Edit	[redacted]	Demo 15	Demo 15 - Edit Rule	Active	03-24-2021 07:51 AM	03-24-2021 - 03-24-2022	Public
View/Edit	[redacted]	Example 16	Example 16 - Share Clinical Lab Data	Draft	03-24-2021 11:23 AM	03-24-2021 - 09-24-2021	Public

Figure 28. Data Access Page (Editing Rules)

6.2 Modify Rule Characteristics and Save

After you click **View/Edit**, you'll be directed to the DATA ACCESS > Edit Rule page (Figure 29) where you will click the **Back/Edit** button to modify the rule.


DATA ACCESS
Edit Rule
Define rule, select users, and select data
Review & Submit Rule
Verify rule contents and set rule status
Back/Edit
Submit
Cancel

Rule Status: Active

Name: Demo 15

Description: Demo 15 - Edit Rule

Access Limit: 03-24-2021 to 03-24-2022

Selected User(s) and Group(s)

Site	User Type	Name
XX	Group	Tropical Storm Barry

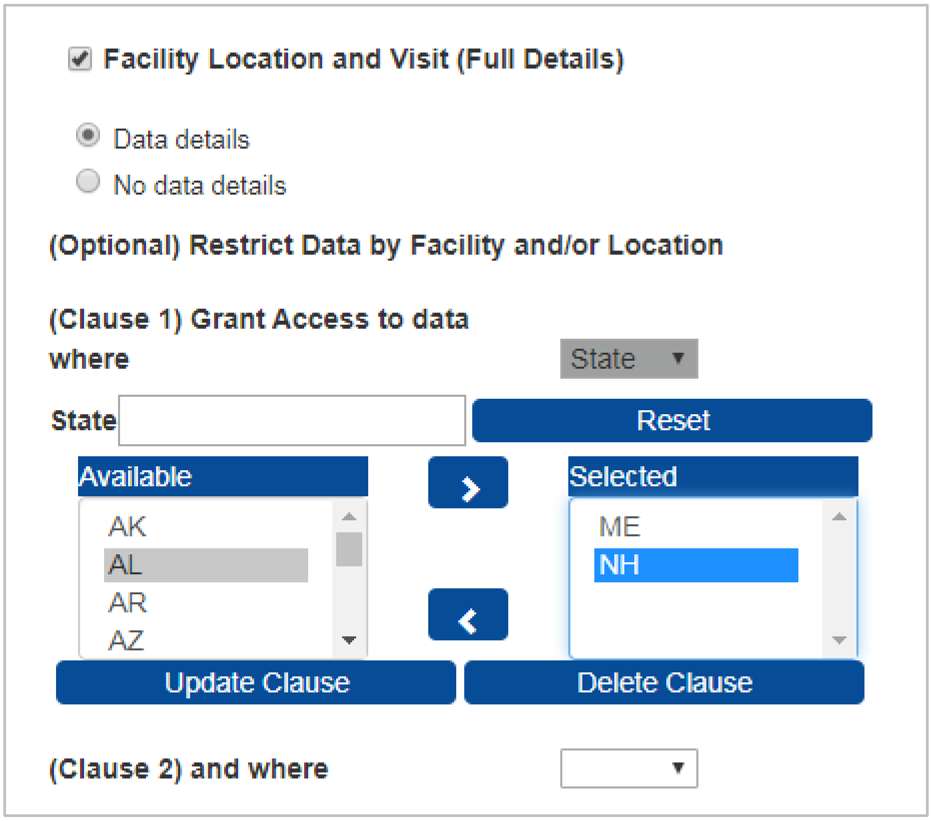
Site	Data Source	Data Details	"WHERE" statement (if applicable)	Delete
XX	Facility Location and Visit (Full Details)	Y	Where County = XX_Bar	X

Figure 29. 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 menu to change a rule's status (e.g., 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 30).



☑ Facility Location and Visit (Full Details)

● Data details

○ No data details

(Optional) Restrict Data by Facility and/or Location

(Clause 1) Grant Access to data where State ▼

State

Available: AK, AL, AR, AZ

Selected: ME, NH

(Clause 2) and where ▼

Figure 30. Data Source Details

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.

6.3 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.

6.3.1 How to Suspend or Deactivate a Rule

Follow these steps to suspend or deactivate a rule:

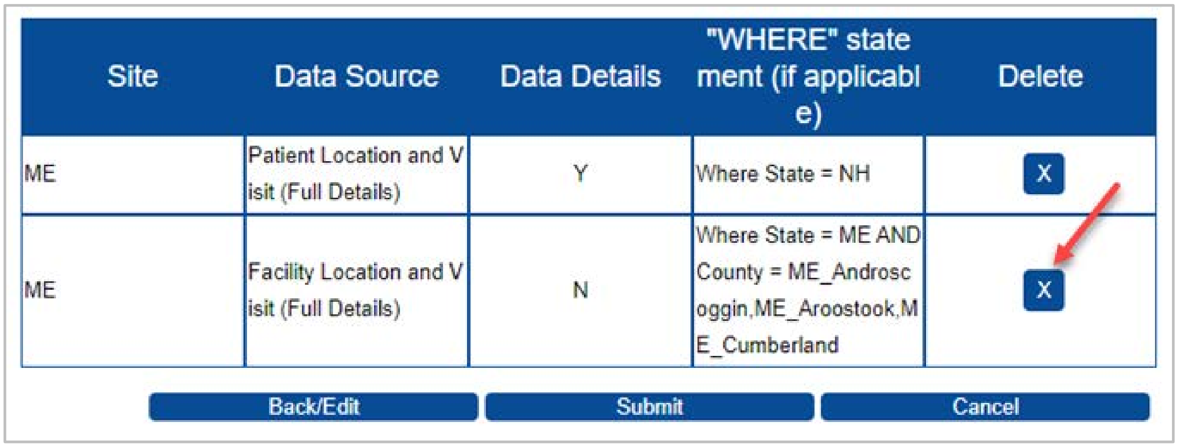
1. Select the rule from the Data Access tab and click **View/Edit**.
2. In the Status drop-down menu, change the value to “Suspend.”
3. Click **Submit**.

6.3.2 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 menu, 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 31).



Site	Data Source	Data Details	"WHERE" statement (if applicable)	Delete
ME	Patient Location and Visit (Full Details)	Y	Where State = NH	X
ME	Facility Location and Visit (Full Details)	N	Where State = ME AND County = ME_Androscoggin,ME_Aroostook,ME_Cumberland	X

Figure 31. Deleting a Rule for a Single Data Source

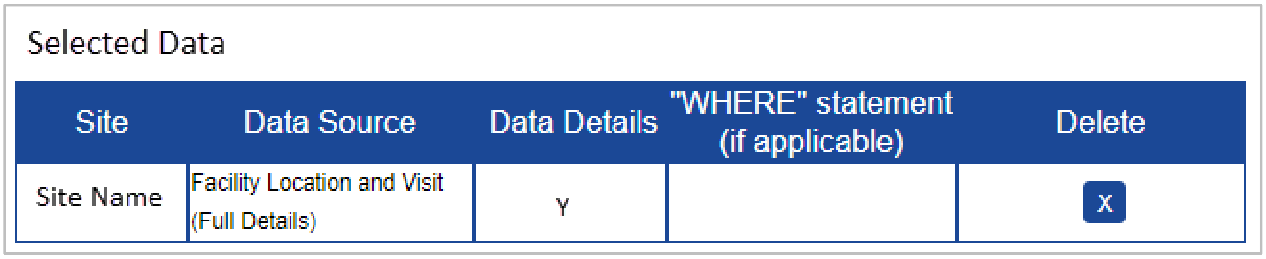
Note: If a rule is suspended, the rule will be removed from the user account(s) in ESSENCE. However, the AMC will preserve the Data Access Rule with a status of “Suspend,” and you may reactivate it later.

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

7. 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 32–37) are some typical ways in which rules govern data being shared.

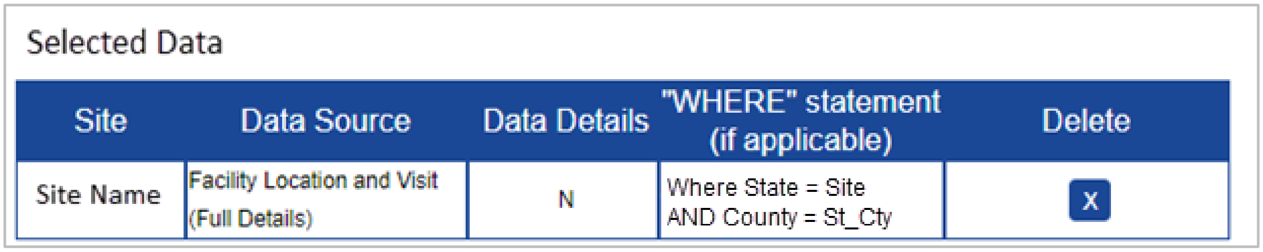
7.1 Facility Location Examples



Selected Data

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

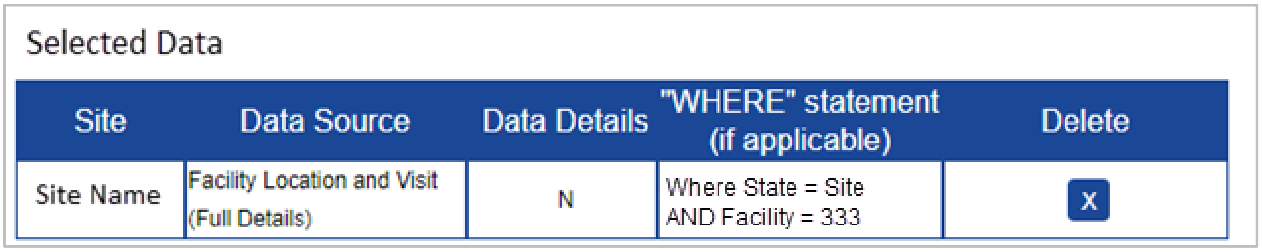
Figure 32. A Site Shares "Facility Location and Visit (Full Details)" Data for All Facilities



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 33. A Site Shares "Facility Location and Visit (Full Details)" Data for a Specific County

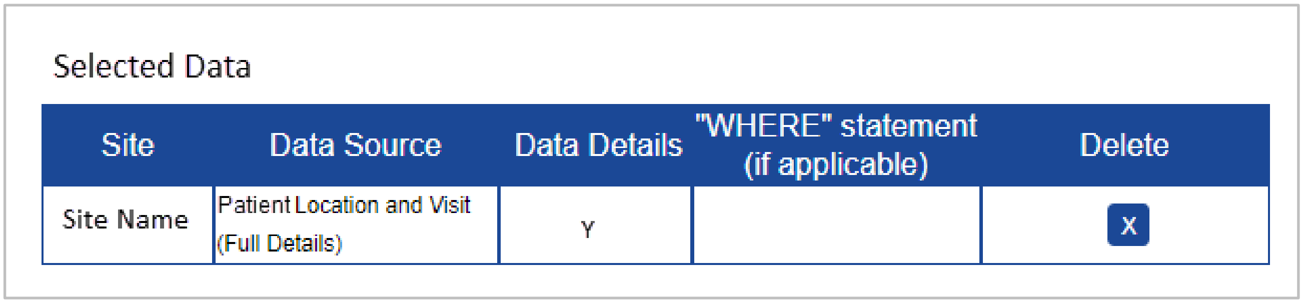


Selected Data

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 34. A Site Shares "Facility Location and Visit (Full Details)" Data for a Specific Facility

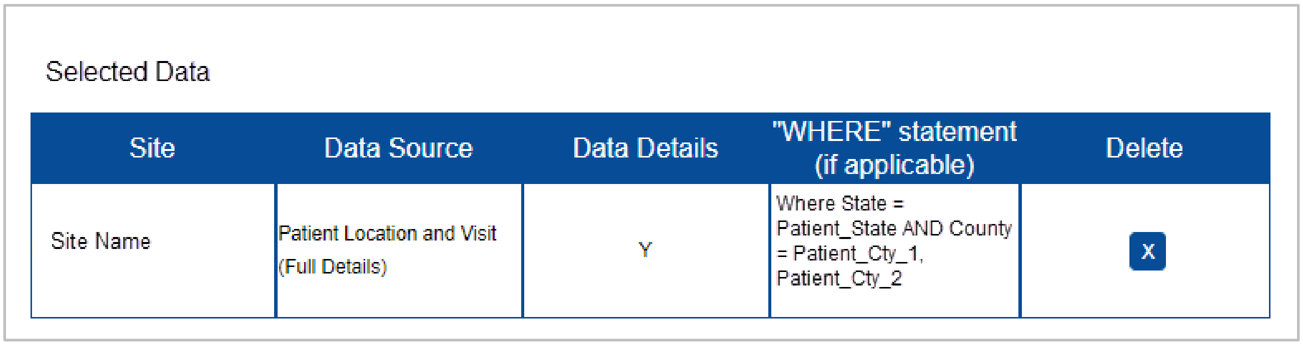
7.2 Patient Location Examples



Selected Data

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

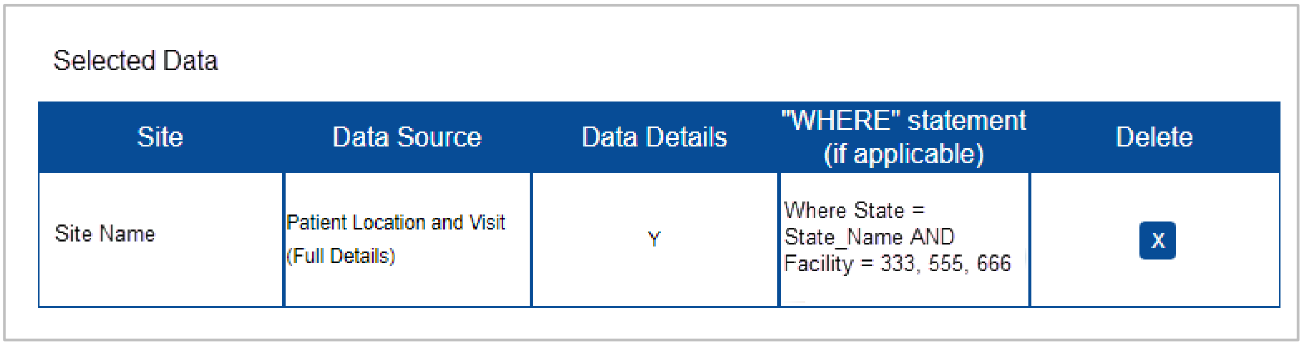
Figure 35. A Site Shares "Patient Location and Visit (Full Details)" with Data Details for Your Site



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

7.3 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, the plus sign (**+**) by "Select a Group" to see the Groups pick list.
5. Scroll down or use the filter field(s) 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 and/or Location" section, choose the "(Clause 1) Grant Access to data where" dropdown and select **State** (Figure 38).

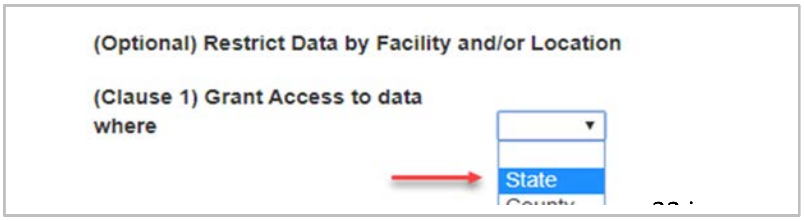

(Optional) Restrict Data by Facility and/or Location
(Clause 1) Grant Access to data where
State
County

Figure 38. Select State for the First WHERE Clause

When you select State, the State pick list is displayed (Figure 39):

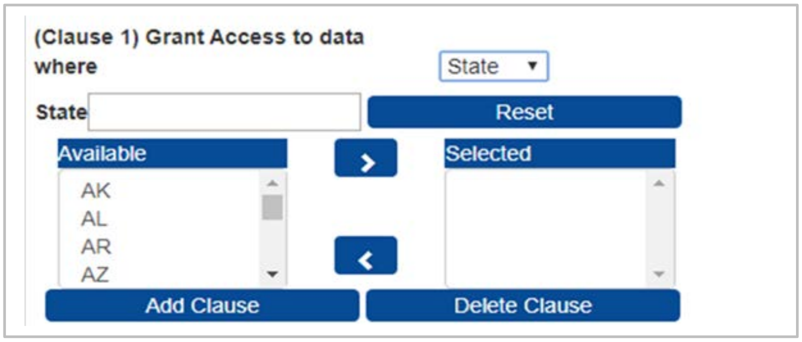


Figure 39. Select your State from Available Pick List

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 dropdown for a second WHERE clause (Figure 40).

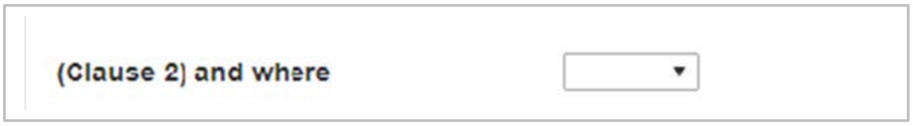

(Clause 2) and where

Figure 40. Select the Second Clause to Filter by County or Counties

11. If you want to limit the counties they can access, then use “Clause 2” and select “County” from the input dropdown. 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 41).

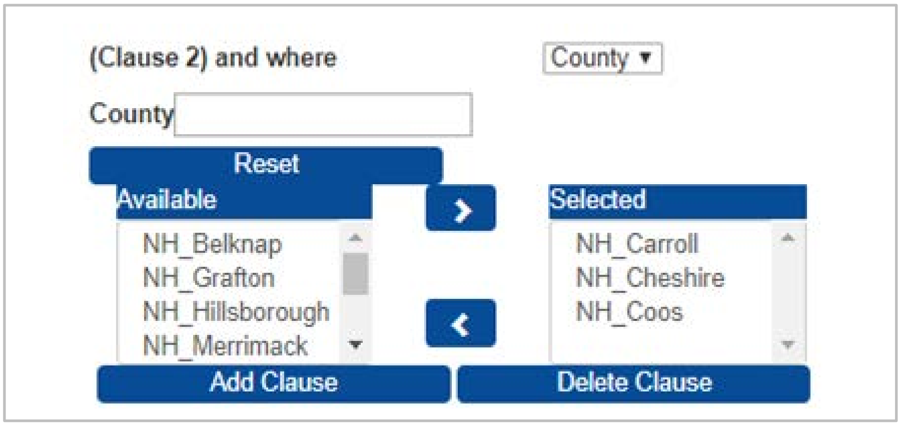

(Clause 2) and where County
County

Figure 41. 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 (e.g., *Where State = NH AND County = NH_Carroll, NH_Cheshire, NH_Coos*). This rule should be saved by using the **Save Draft, Next, or Save/Submit** button.

13. When satisfied, set the rule to Active and click the **Submit** button. The user or users in New Hampshire will be able to view the data based on the source and data level in the county or counties you selected.

Step 4: Review and Save the Rule

Do's and Don'ts of Data Sharing Rules in the AMC

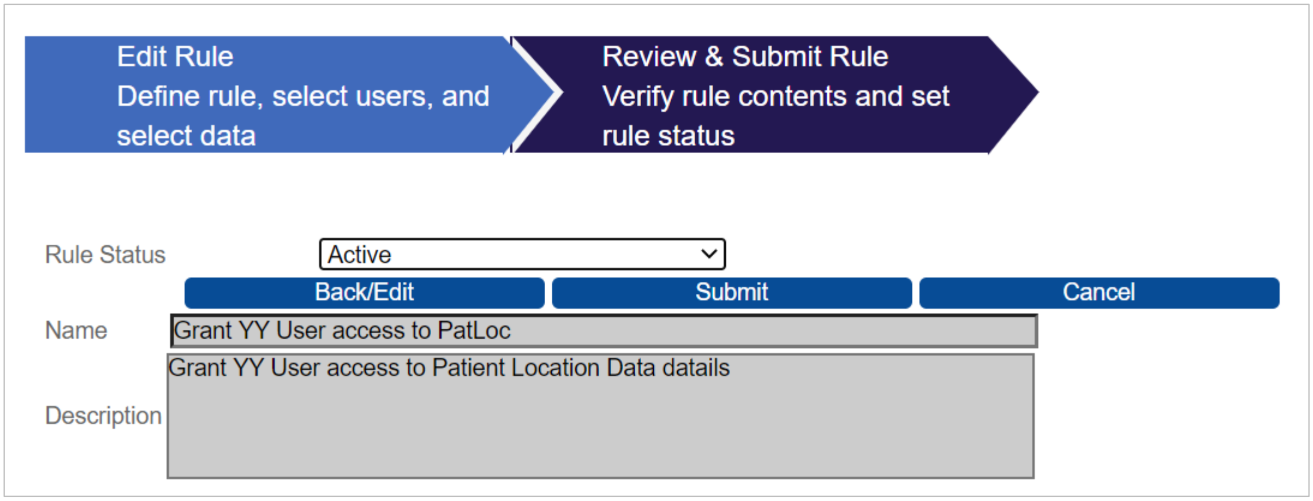
1. You *can* share data with other users in your site and restrict by a patient's location using the "By Patient Location" data sources.
2. When sharing data with users outside your site, we recommend you *do not* share by patient location because ESSENCE will consolidate that rule with other patient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

Once you name your rule and select users and data, you're ready to save and implement your Data Access Rule (Figure 42).

First, confirm that your selections are as expected. Use the edit buttons to modify the information displayed. Next, **select the appropriate status for your rule** (note that 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.

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


Edit Rule
Define rule, select users, and select data
Review & Submit Rule
Verify rule contents and set rule status
Back/Edit
Submit
Cancel

Rule Status: Active

Name: Grant YY User access to PatLoc

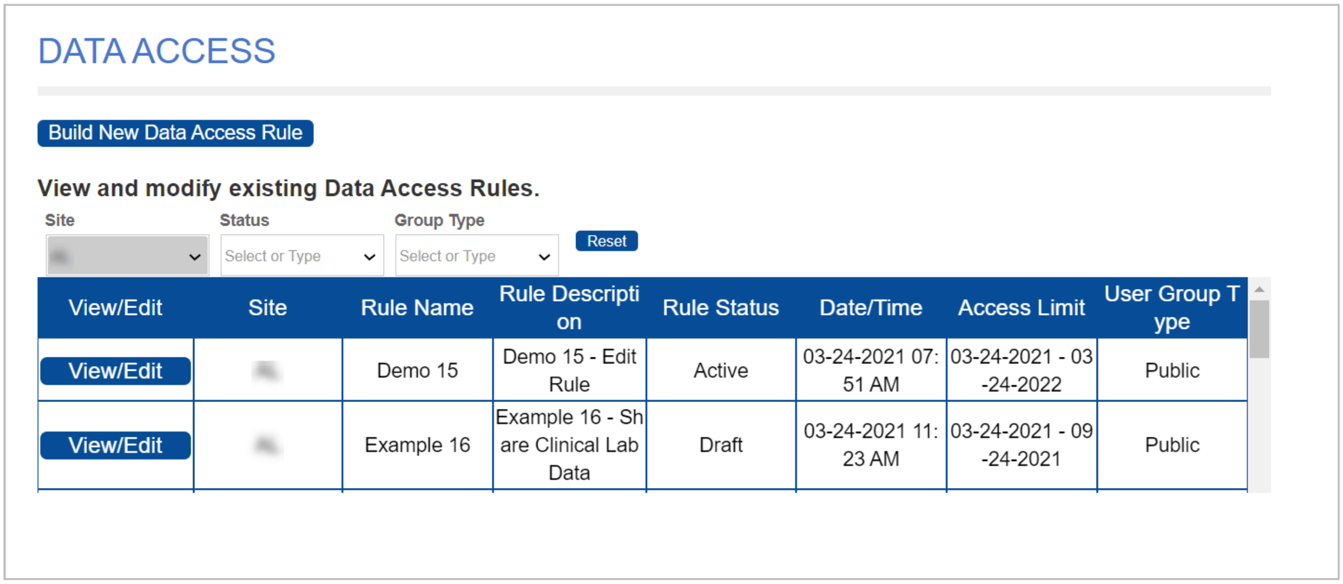
Description: Grant YY User access to Patient Location Data datails

Figure 42. Data Access Page (Review & Submit Rule)

7.4 Example of Editing a Rule

Step 1: Select a Rule

On the Data Access tab under View/Edit, click the **View/Edit** button beside the rule you want to edit (Figure 43).



DATA ACCESS

View and modify existing Data Access Rules.

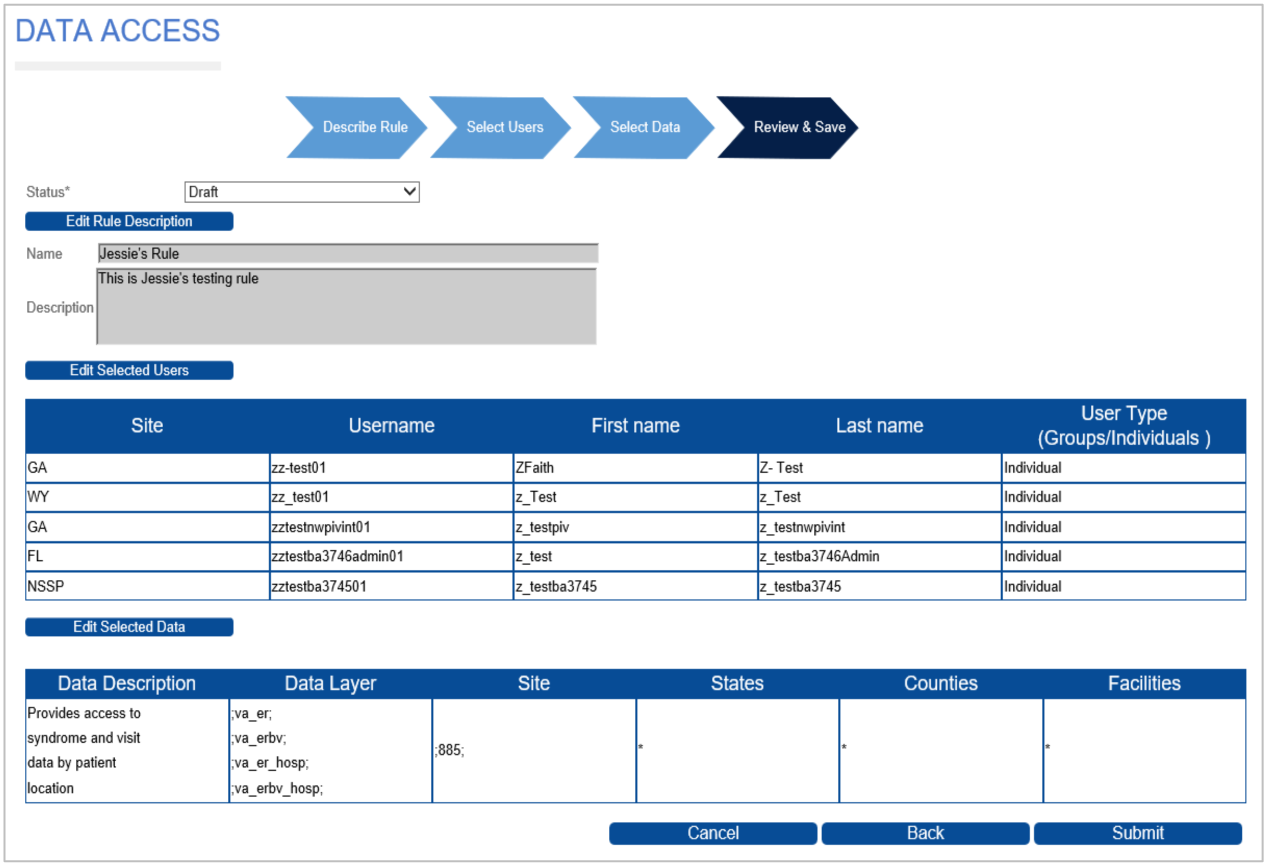
Site: [redacted]
Status: Select or Type
Group Type: Select or Type

View/Edit	Site	Rule Name	Rule Description	Rule Status	Date/Time	Access Limit	User Group Type
View/Edit	[redacted]	Demo 15	Demo 15 - Edit Rule	Active	03-24-2021 07:51 AM	03-24-2021 - 03-24-2022	Public
View/Edit	[redacted]	Example 16	Example 16 - Share Clinical Lab Data	Draft	03-24-2021 11:23 AM	03-24-2021 - 09-24-2021	Public

Figure 43. 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 44). Use the "Edit" buttons to change rule information, users, or data. You can also use the status drop-down menu to change a rule's status. When you finish modifying your Data Access Rule, click **Submit**.



DATA ACCESS

Status* Draft

Name: Jessie's Rule

Description: This is Jessie's testing rule

Site	Username	First name	Last name	User Type (Groups/Individuals)
GA	zz-test01	ZFaith	Z- Test	Individual
WY	zz_test01	z_Test	z_Test	Individual
GA	zztestnwpivint01	z_testpiv	z_testnwpivint	Individual
FL	zztestba3746admin01	z_test	z_testba3746Admin	Individual
NSSP	zztestba374501	z_testba3745	z_testba3745	Individual

Data Description	Data Layer	Site	States	Counties	Facilities

Provides access to syndrome and visit data by patient location	;va_er;
	;va_erbv;
	;va_er_hosp;
	;va_erbv_hosp;
		;885;	*	*	*

Figure 44. Editing Rules (Review & Save)

7.5 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 (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 (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 of 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:

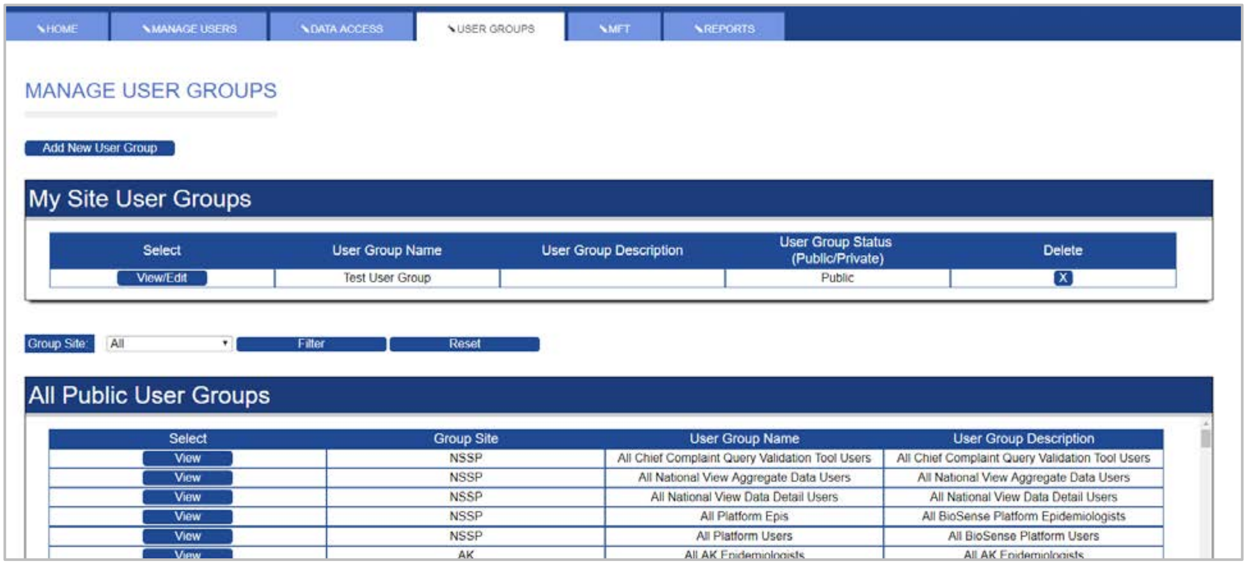
John's access after the rule…	Site	State	County	Data source *(ESSENCE Variable Name)*	Facility

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

8. User Groups

The User Groups tab is only available to site administrators (Figure 45). User groups are a convenient way to add multiple users to data access rules instead of adding individual users one-by-one. Site administrators may create any number of public or private user groups. *Public user groups* are viewable and usable by other site's administrators to add to their data access rules. *Private user groups* are only viewable and usable by that site's administrators. Once a user group is created, that user group will be assignable to data access rules.



MANAGE USER GROUPS

My Site User Groups

Select	User Group Name	User Group Description	User Group Status (Public/Private)	Delete
View/Edit	Test User Group		Public	X

All Public User Groups

Select	Group Site	User Group Name	User Group Description
View	NSSP	All Chief Complaint Query Validation Tool Users	All Chief Complaint Query Validation Tool Users
View	NSSP	All National View Aggregate Data Users	All National View Aggregate Data Users
View	NSSP	All National View Data Detail Users	All National View Data Detail Users
View	NSSP	All Platform Epis	All BioSense Platform Epidemiologists
View	NSSP	All Platform Users	All BioSense Platform Users
View	AK	All AK Epidemiologists	All AK Epidemiologists

Figure 45. User Groups Page—View/Edit My Site User Groups—View Public User Groups

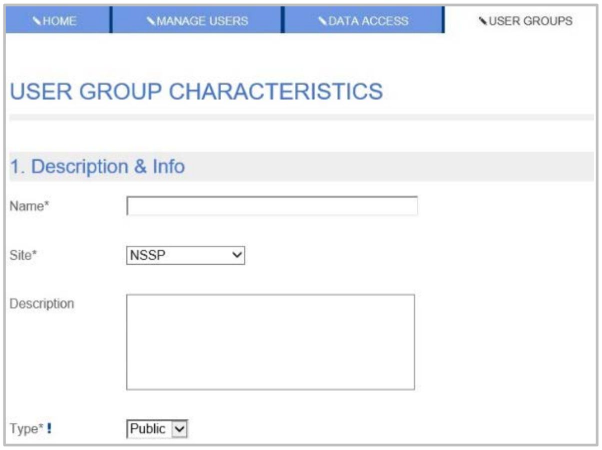
8.1 Create a New User Group

Step 1: Select User Group Characteristics

Click the **Add New User Group** button on the main User Groups page. Enter the user group's characteristics (Figure 46). Create a unique name for the user group, add a description, and select a type (public or private) for the group. Provide enough detail so that you can quickly distinguish user groups from each other. Note that Site will show the logged-in user's site and cannot be changed.

Group Types: There are currently two types of groups:

- ***Public***—All users who are authorized to manage user groups (typically site administrators) can see the group. Since this will be listed in the All Public User Groups table on the main User Groups page, consider including your site abbreviation or short name in the name. **Note:** The All Public User Groups table displays all public groups in the *system*, not just your site.
- ***Private***—Only users (site administrators) who are associated with the site that owns and controls the group will see the user group.



USER GROUP CHARACTERISTICS

1. Description & Info

Name*

Site* NSSP

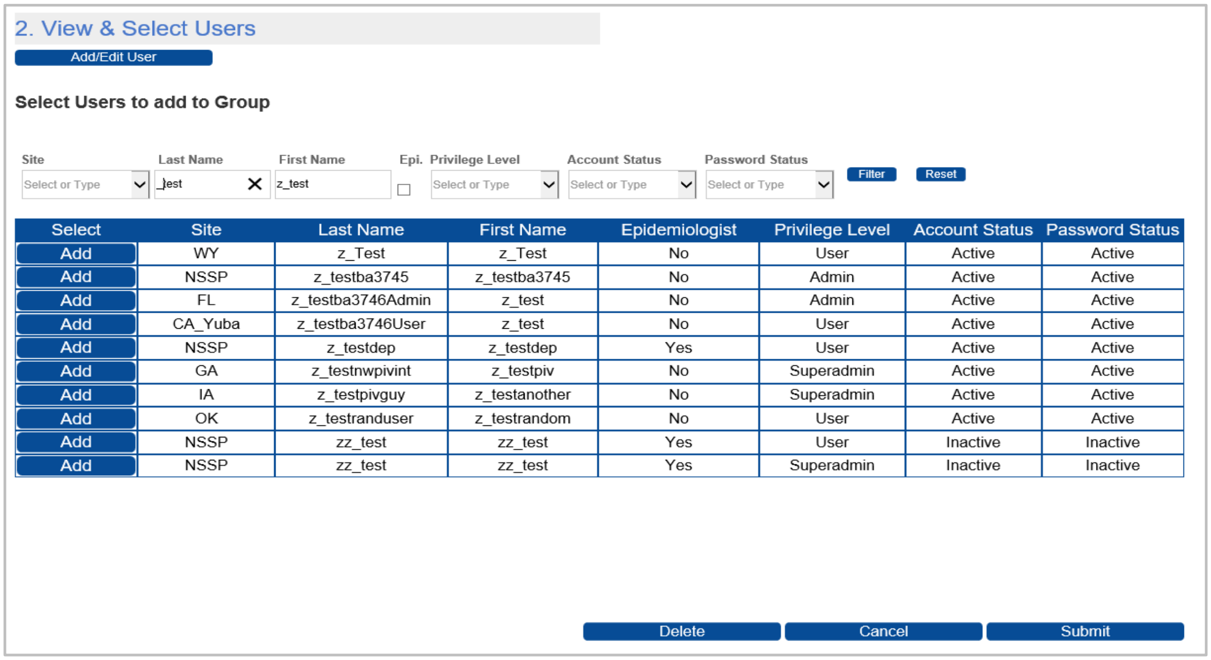
Description

Type* ! Public

Figure 46. User Group Description and Information

Step 2: Select Users

Click the **Add/Edit User** button to add users to the group (Figure 47). At least one user is required to submit the group. Remember that any users selected here will receive access to the data you specify when you create your data access rules. Use the filters to locate users to add to the group. Adding users is simplified with one click of the “Add” button next to the user’s name. When you’ve completed adding users, click the **Submit** button to save the group. Now, your group is active.



2. View & Select Users

Select Users to add to Group

Site	Last Name	First Name	Epi.	Privilege Level	Account Status	Password Status
Select or Type	_test	z_test	□	Select or Type	Select or Type	Select or Type

Select	Site	Last Name	First Name	Epidemiologist	Privilege Level	Account Status	Password Status
Add	WY	z_Test	z_Test	No	User	Active	Active
Add	NSSP	z_testba3745	z_testba3745	No	Admin	Active	Active
Add	FL	z_testba3746Admin	z_test	No	Admin	Active	Active
Add	CA_Yuba	z_testba3746User	z_test	No	User	Active	Active
Add	NSSP	z_testdep	z_testdep	Yes	User	Active	Active
Add	GA	z_testnwpivint	z_testpiv	No	Superadmin	Active	Active
Add	IA	z_testpivguy	z_testanother	No	Superadmin	Active	Active
Add	OK	z_testranduser	z_testrandom	No	User	Active	Active
Add	NSSP	zz_test	zz_test	Yes	User	Inactive	Inactive
Add	NSSP	zz_test	zz_test	Yes	Superadmin	Inactive	Inactive

Figure 47. User Groups Page (View & Select Users)

8.2 Edit a User Group

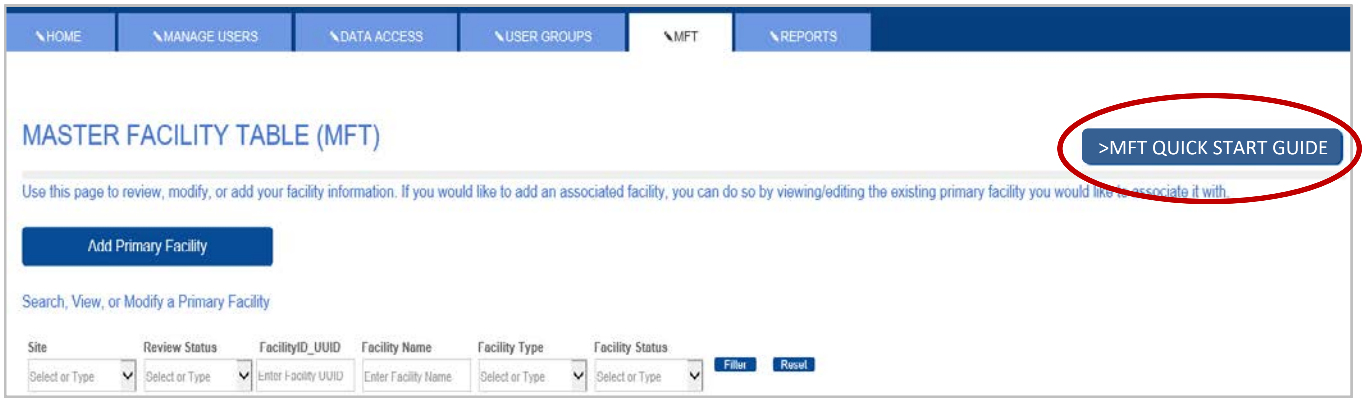
Site administrators may edit the site-specific user groups they create. Examples include changing the group name, changing the group to *public* or *private*, and adding or removing group members. The site administrator may also delete a group that is no longer needed.

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

Members of the user group cannot view ESSENCE syndromic surveillance data UNLESS the group has, at least, one data access rule or has data access rules associated with their user ID or are members of other groups with data access rules.

9. Master Facility Table

The Master Facility Table (MFT) resides within the AMC and provides an interface for site administrators and the NSSP onboarding staff to use throughout the multistage onboarding process. For in-depth instructions, the *BioSense Platform Quick Start Guide to Using the Master Facility Table* can be accessed by clicking the button in the upper right-hand corner of the MFT tab (Figure 48).



MASTER FACILITY TABLE (MFT)

Use this page to review, modify, or add your facility information. If you would like to add an associated facility, you can do so by viewing/editing the existing primary facility you would like to associate it with.

Search, View, or Modify a Primary Facility

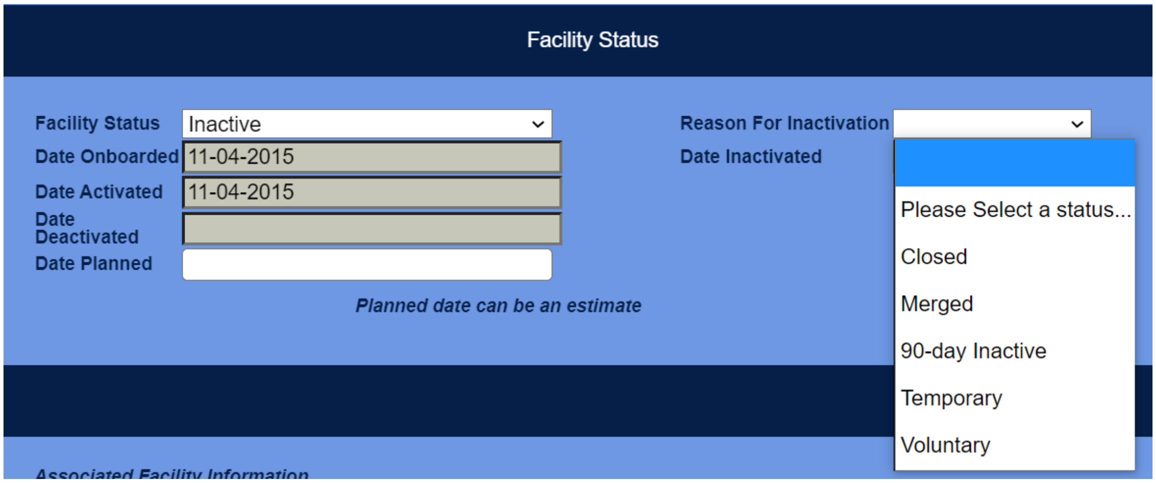
Site	Review Status	FacilityID_UUID	Facility Name	Facility Type	Facility Status
Select or Type	Select or Type	Enter Facility UUID	Enter Facility Name	Select or Type	Select or Type

Figure 48. Master Facility Table (MFT) Page

9.1 Facility Inactivation Reason and Date

The options for making facilities inactive have been standardized by adding dropdown lists for Reason For Inactivation and the Date Inactivated fields (Figure 49). 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



Facility Status

Facility Status	Inactive
Date Onboarded	11-04-2015
Date Activated	11-04-2015
Date Deactivated	
Date Planned	
Reason For Inactivation	
Date Inactivated	

Planned date can be an estimate

Figure 49. When Facility Status is Changed to Inactive, the Reason for Inactivation Dropdown 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 status; 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.

9.2 Facilities in U.S. Territories

Facilities in the U.S. Territories can now be added to the Master Facility Table. American Samoa, Guam, Northern Mariana Islands, Puerto Rico, and the U.S. Virgin Islands are now available in the "State" dropdown list.

Here are the territories with their "State" abbreviations:

Table 1. U.S. Territory State Abbreviations

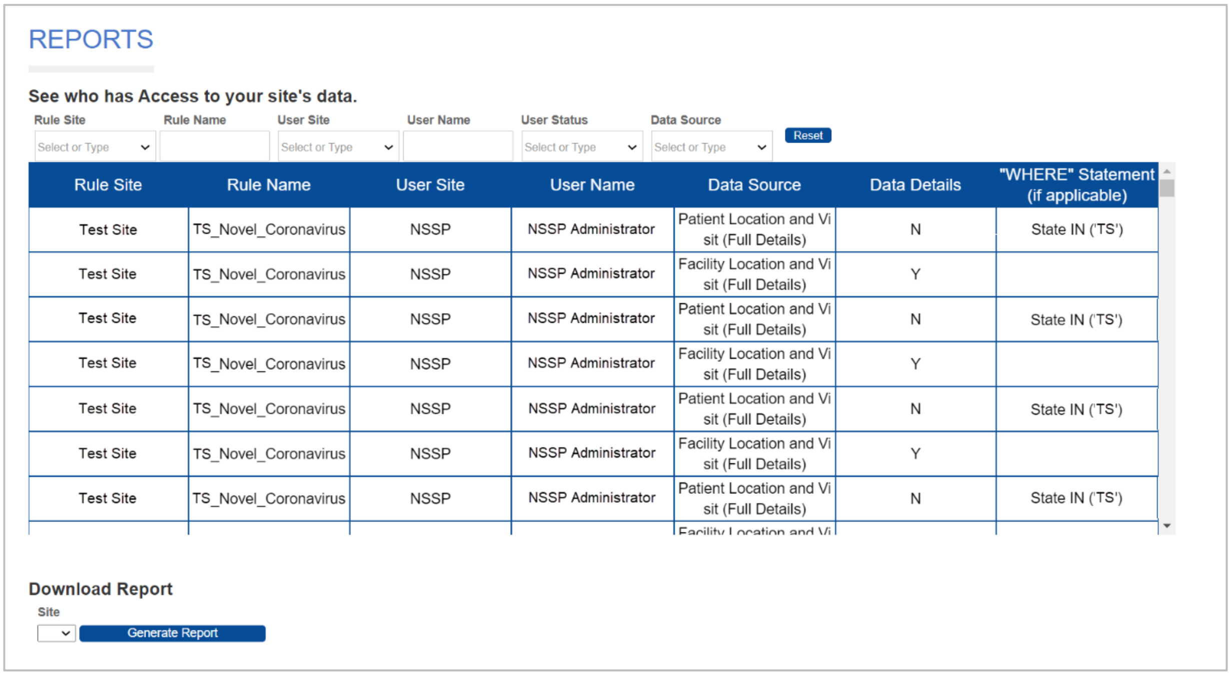
U.S Territory	State Abbreviation
American Samoa	AS
Guam	GU
Northern Mariana Islands	MP
Puerto Rico	PR
U.S. Virgin Islands	VI

Once the State field is populated, the County dropdown will provide applicable counties that can be selected.

10. Reports

The Reports tab (Figure 50) is only available to site administrators. This tab provides a table of all the data access rules that affect the site's users, as well as users from other sites who have been granted access. The tab displays the rule name and site, the user ID and name of the user granted access and his or her site, 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.

Rules affecting the site that have been created by NSSP are also listed. Note that it can take up to a minute or more for this tab to fully load. Please be patient.



REPORTS

See who has Access to your site's data.

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')
				Facility Location and Vi		

Download Report

Figure 50. Data Access Reports Page

The Reports tab includes filters for the following report columns:

- Rule Site—Allows site administrators to select only their own site to 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 *
- 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 are for "awend01 (Alice Wend)" and you enter "alic" in the User Name search field, all rules for both these users will be displayed.

Also note that the report can be filtered by User Status (Active or Inactive). This allows site administrators to filter out rules granting access to inactive users, or to view only inactive users.

A full report is available for download to 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.

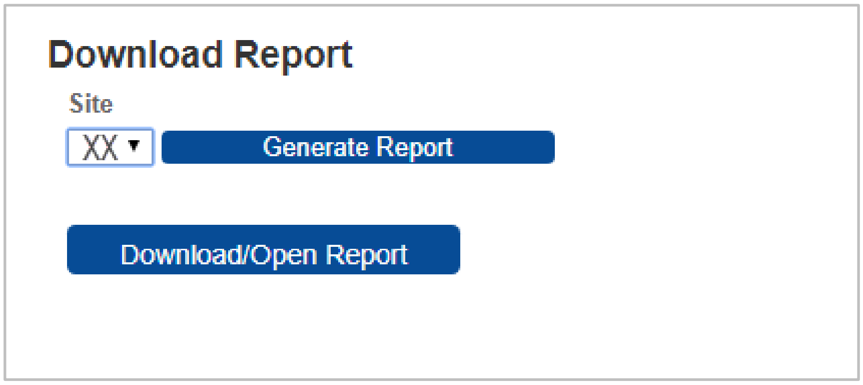


Figure 51. Data Access Reports Page—Generate Report

The "Generate Report" button in the lower left of the Reports tab page (Figure 51) has a Site selection dropdown list so you can select a report with just your site's rules. By leaving the Site field blank, all rules including the Operational Access and NSSP rules will be in the report.

If desired, select the short name abbreviation for your site as a filter (Default [blank] selects all rules), then click the **Generate Report** button. After a few moments, the "Download/Open Report" button will be displayed (Figure 51). Once you click the **Download/Open Report** button, the report (in CSV format) will be downloaded to your Download folder. You may open it directly from your browser by clicking on the downloaded file button at the bottom left, or you may directly access the file in your Download folder using Windows.

11. 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.

11.1 Site Administrators

1. Log in with provided credentials.
   a. Accept the Site Administrator Code of Conduct.
   b. Change user password.
2. View and edit user profile information.
3. Create a user in their site.
4. Create a user group for their site.
5. View existing users within their site.
6. Edit users within their site.
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 they have created in their site. Site administrators may also grant access to users from other sites. When creating Data Access Rules, we recommend that you confirm with the user that the Data Access Rule results in the desired permissions in ESSENCE.

11.2 Users

1. In the My Info section, users can:
   a. Accept the Code of Conduct.
   b. Change their passwords.
   c. View and edit their profile information.
2. In the NSSP Applications section, users can link directly to:
   a. ESSENCE
   b. RStudio Pro (SQL Query)
   c. SAS Studio
   d. Data Quality Dashboards

   Note: Access depends on user profile setup and specific login privileges.
3. 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