

## **Access Policies**

# Contents

**Access Policies..... 3**

    View Existing Access Policies..... 3

    Create an Access Policy..... 4

    View Access Policy Information..... 5

    Modify an Access Policy..... 6

    Delete an Access Policy..... 8

## Access Policies

---

Access policies let you characterize rightful access in terms of user authorizations and data sensitivity, or visibility.

An access policy is a set of logical rules that determines how users can consume data stored in PHEMI Central. The access policy specifies what user authorizations are required to interact with data tagged with specified sensitivity, or visibility. Access policies can be applied to data sources and datasets.

To create an access policy, you define one or more access rules. Each rule has three parts.

- Subject specifies who may access the data. Access is characterized in terms of user authorizations. [Tell me about user authorizations.](#)
- Action specifies what action authorized users may take to interact with the data.
- Object specifies the kind of data for which the access is being granted. The data is specified in terms of data visibility. [Tell me about data visibilities.](#)

A rule is matched when the user making the request has an authorization matching at least one of those listed for Subject, and the data being requested has a visibility matching at least one of those listed for Object. When there is a match, the user may take the specified action(s) on the data.

If there is more than one rule in an access policy, the rules are related by OR logic.

The rules in a given access policy are intended to implement specific controls over data. Depending on the number and kinds of datasets your organization works with, you may need just one access policy or multiple access policies.

If you have multiple access policies, it is possible for policies to conflict with one another and still represent a consistent governance policy, provided that each access policy is used to control different data sources or datasets. For example, one access policy may allow users with Researcher authority to read CONFIDENTIAL data while another access policy does not. This can be perfectly consistent, given the policies control different data.

## View Existing Access Policies

---

See what access policies have been configured on the **Access Policy Builder** page.

To view defined access policies:

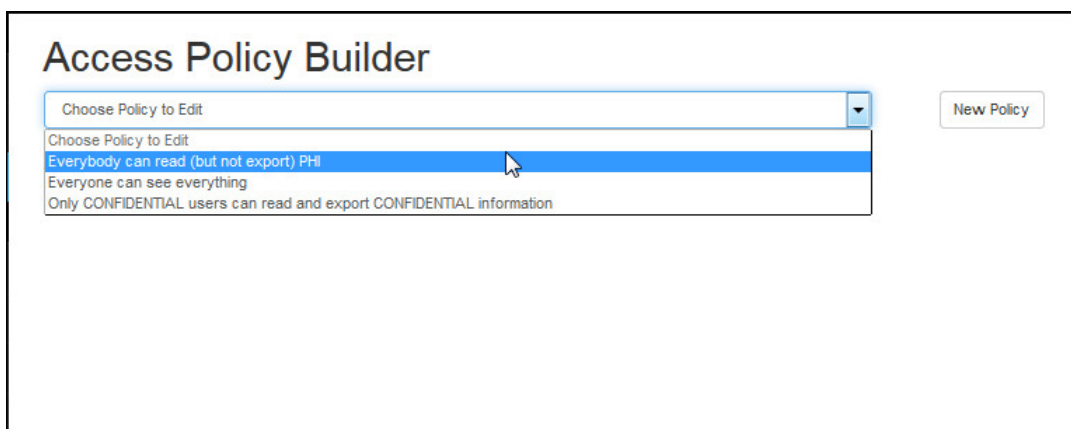
1.

Open the **Access Policy Builder** page, by clicking the **Access Policy Builder** icon in the left navigation bar.



The **Access Policy Builder** page opens.

2. At the right of the **Choose Policy to Edit** field, click the drop-down arrow to see the list of configured access policies.



## Create an Access Policy

Create a new access policy on the **Access Policy Builder** page.

Before you can create an access policy you must configure the following:

- User authorizations [How do I configure user authorizations?](#)
- Data visibilities [How do I configure data visibilities?](#)

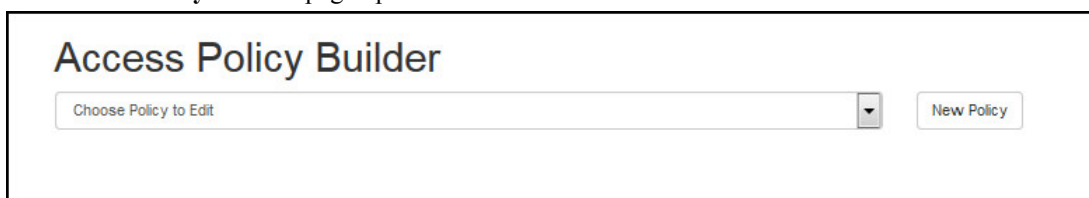
To create a new access policy, define one or more access rules:

1.

Open the **Access Policy Builder** page, by clicking the **Access Policy Builder** icon in the left navigation bar.



The **Access Policy Builder** page opens.



2. Click the **New Policy** button.

The form for the new access policy opens, with Rule 1 ready for you to edit.

3. Enter the access rule information.

Option	Description
--------	-------------

<b>Subject</b>	Mandatory. The user authorizations allowed to perform the action on the data. User authorizations are configured for the system by the administrator.
----------------	---

<b>Action</b>	Mandatory. The action(s) an authorized user may take on the data. Supported actions are as follows: <ul style="list-style-type: none"> <li>• Read. The user may view the data.</li> <li>• Export. The user may export the data to a destination, such as a local computer for analysis.</li> </ul>
---------------	--

<b>Object</b>	Mandatory. The data visibilities authorized users are allowed to access. Data visibilities are configured by the administrator.
---------------	---

4. Add another rule by clicking the **Add Rule** button. Or, save the access policy by clicking the **Save Access Policy** button. The system confirms when the access policy has been successfully saved.

## View Access Policy Information

View the information configured for a given access policy on the **Access Policy Builder** page.

To view information for an access policy:

1.

Open the **Access Policy Builder** page, by clicking the **Access Policy Builder** icon in the left navigation bar.



The **Access Policy Builder** page opens.

- At the right of the **Choose Policy to Edit** field, click the drop-down arrow to see configured access policies. Select the policy you want to view.

**Access Policy Builder**

Choose Policy to Edit

Choose Policy to Edit

Everybody can read (but not export) PHI

Everyone can see everything

Only CONFIDENTIAL users can read and export CONFIDENTIAL information

New Policy

The screen for the selected access policy opens, showing the information configured for it.

**Access Policy Builder**

Only CONFIDENTIAL users can read and export CONFIDENTIAL information

New Policy

Name Only CONFIDENTIAL users can read and export CONFIDENTIAL information

Rule 1

Subject CONFIDENTIAL

Action CAN Read, Export

Object CONFIDENTIAL

Add Rule

Delete Access Policy

Save Access Policy

## Modify an Access Policy

Modify an access policy on the **Access Policy Builder** page.

To modify an access policy:

- 1.

Open the **Access Policy Builder** page, by clicking the **Access Policy Builder** icon in the left navigation bar.



The **Access Policy Builder** page opens.

**Access Policy Builder**

Choose Policy to Edit ▼

New Policy

- At the right of the **Choose Policy to Edit** field, click the drop-down arrow to see configured access policies. Select the policy you want to modify.

**Access Policy Builder**

Choose Policy to Edit ▼

- Choose Policy to Edit
- Everybody can read (but not export) PHI
- Everyone can see everything
- Only CONFIDENTIAL users can read and export CONFIDENTIAL information

New Policy

The screen for the selected access policy opens, showing the information configured for it.

**Access Policy Builder**

Only CONFIDENTIAL users can read and export CONFIDENTIAL information ▼

New Policy

Name Only CONFIDENTIAL users can read and export CONFIDENTIAL information

**Rule 1** 🗑️

<b>Subject</b>		<b>Action</b>
CONFIDENTIAL ▼	CAN	Read, Export ▼
<b>Object</b>		
CONFIDENTIAL ▼		

Add Rule

Delete Access Policy Save Access Policy

- Do any of the following.
  - Modify an existing rule by editing values for Subject, Action, or Object.
  - Add a new rule by clicking the **Add Rule** button and populating the fields.
  - Delete a rule by clicking the trash can icon to the right of the rule.
- Click the **Save Access Policy** button to save the changes.

## Delete an Access Policy

Delete an access policy on the **Access Policy Builder** page.

To delete an access policy:

1.

Open the **Access Policy Builder** page, by clicking the **Access Policy Builder** icon in the left navigation bar.



The **Access Policy Builder** page opens.

2. At the right of the **Choose Policy to Edit** field, click the drop-down arrow to see configured access policies. Select the policy you want to modify.

The screen for the selected access policy opens, showing the information configured for it.



3. Click the **Delete Access Policy** button. The system asks you to confirm deletion; click **Delete**.