Data Visibilities

Contents

Data Visibilities

Data visibilities identify the privacy requirements for data.

All raw data and derived data stored in PHEMI Central can be tagged with labels that provide information about the data's sensitivity. This sensitivity is described in terms of the visibility the data should have to different system users. The visibility tags you define for your data should reflect the sensitivity of the data as identified by your organization.

The visibility of data in your organization should be set out in your organization's governance policy. Working from the governance policy, the PHEMI Administrator and is configured as part of system configuration.

PHEMI Central comes with three data visibilities predefined.

Table 1: Predefined Data Visibilities

Visibility	Meaning
IDENTIFIED	Sensitive data that contains identifying information. Such data should be secured and available only to authorized personnel.
DE_IDENTIFIED	Sensitive data that has been transformed and masked to remove identifying information
NONIDENTIFIED	Data that does not contain sensitive or identifying data.

You can define additional data visibilities to suit your organization's needs. Possible examples are CONFIDENTIAL to identify data that is sensitive and requires a user to a certain level of access or certification to access, PII to identify Personally Identifiable Information, PHI to identify personal health information, or SECRET to identify especially sensitive material.

Note: Once defined, a data visibility may be neither edited nor deleted. The description for the visibility can be modified subsequently.

The data visibilities specified for a data source are referred to in access policies and matched against user authorizations to determine what actions, if any, a given user is allowed to perform on the data. The access policy can then be applied to a data source or dataset during system configuration. *Tell me about user authorizations. Tell me about access policies.*

In addition, any data visibility defined in the system can be used by a Data Processing Function (DPF) to tag any derived data fields. These derived data elements can be assigned different privacy levels from the data source and from one another. For example, the Social Security Number extracted from a health record can be tagged CONFIDENTIAL if that data visibility has been defined in the system. This mechanism provides field-level privacy protection.

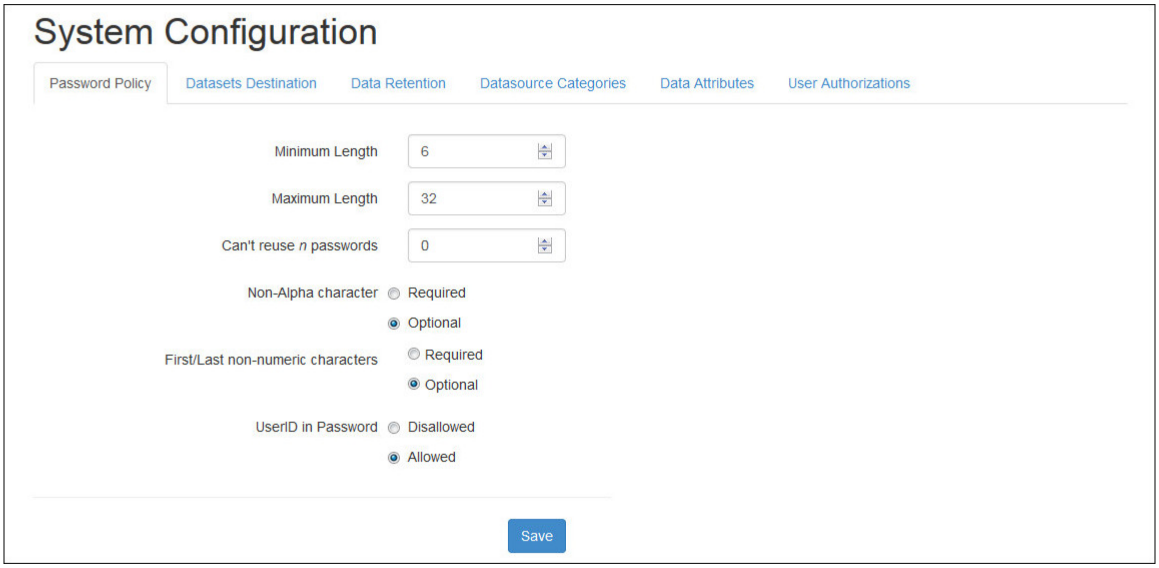
View Configured Data Visibilities

View configured data visibilities on the **System Configuration** page.

To view the data visibilities that have been configured in the system:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

   The **System Configuration** page opens on the **Password Policy** screen.



System Configuration

Minimum Length: 6

Maximum Length: 32

Can't reuse *n* passwords: 0

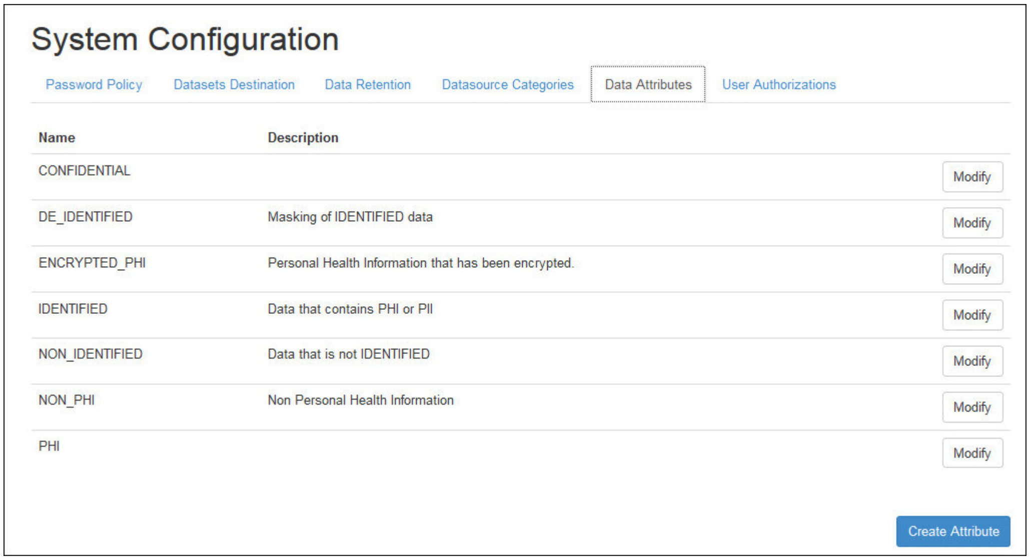
Non-Alpha character: ○ Required ● Optional

First/Last non-numeric characters: ○ Required ● Optional

UserID in Password: ○ Disallowed ● Allowed

2. Click the **Data Attributes** tab.

The **Data Attributes** screen opens, listing all the data visibilities configured for the system.



System Configuration

Name	Description	
CONFIDENTIAL		Modify
DE_IDENTIFIED	Masking of IDENTIFIED data	Modify
ENCRYPTED_PHI	Personal Health Information that has been encrypted.	Modify
IDENTIFIED	Data that contains PHI or PII	Modify
NON_IDENTIFIED	Data that is not IDENTIFIED	Modify
NON_PHI	Non Personal Health Information	Modify
PHI		Modify

Define Data Visibilities

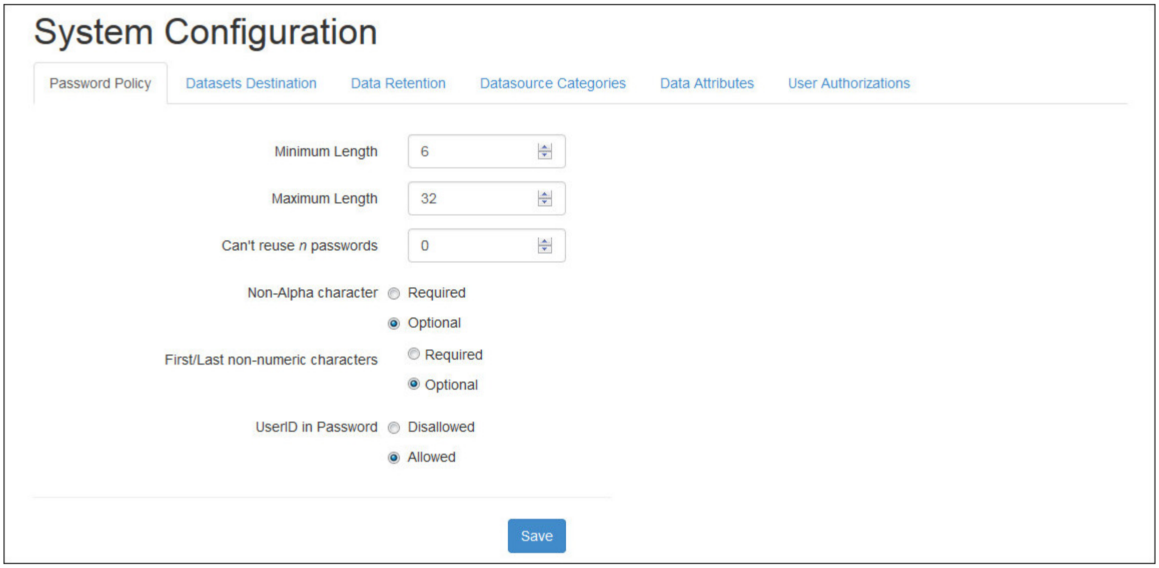
Define data visibilities on the **System Configuration** page.

Note: Once defined, a data visibility may be neither edited nor deleted. The description may be modified subsequently.

To define data visibilities:

1. Open the **System Configuration** page, by clicking the **System Configuration** icon in the left navigation bar.

The **System Configuration** page opens on the **Password Policy** screen.



System Configuration

Minimum Length: 6

Maximum Length: 32

Can't reuse *n* passwords: 0

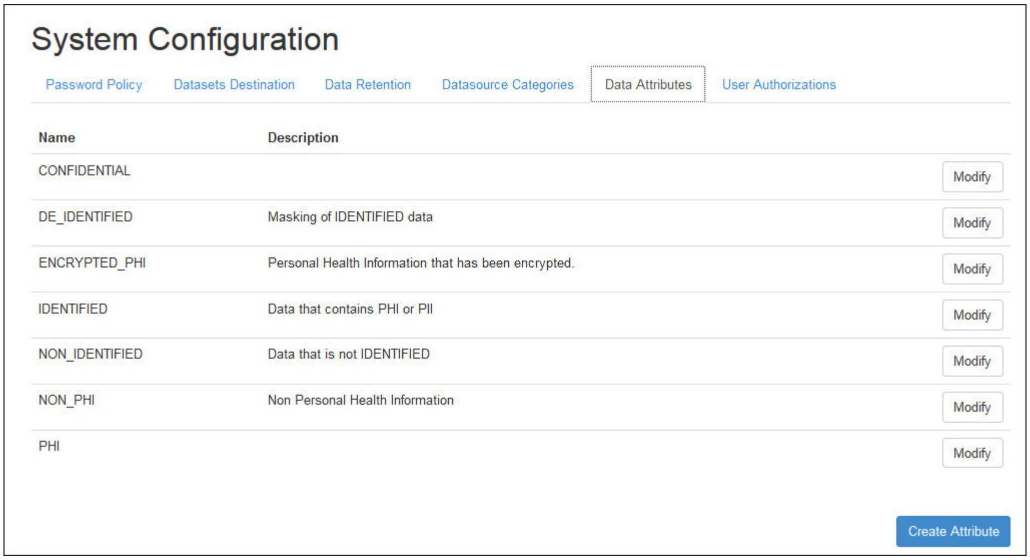
Non-Alpha character: ○ Required ● Optional

First/Last non-numeric characters: ○ Required ● Optional

UserID in Password: ○ Disallowed ● Allowed

2. Click the **Data Attributes** tab.

   The **Data Attributes** screen opens.



System Configuration

Name	Description	
CONFIDENTIAL		Modify
DE_IDENTIFIED	Masking of IDENTIFIED data	Modify
ENCRYPTED_PHI	Personal Health Information that has been encrypted.	Modify
IDENTIFIED	Data that contains PHI or PII	Modify
NON_IDENTIFIED	Data that is not IDENTIFIED	Modify
NON_PHI	Non Personal Health Information	Modify
PHI		Modify

3. Click the **Create Attribute** button. The **Create Attribute** screen opens.
4. Enter the visibility information.

Option	Description
Name	Enter a name for the data visibility; for example, "CONFIDENTIAL," "SECRET" or "PII".
Description	Enter a brief description to describe the intention of the visibility.

5. Save the visibility information by clicking the **Create Attribute** button.