Introducing PHEMI Central

Contents

Introducing PHEMI Central

To be written

Intro blurb to segue into following overview content.

Overview

To be written.

This topic will provide a basic introduction to and overview of the system. It will include relevant content and diagrams similar to that in the Product Description currently being developed.

Data in

To be written.

This topic will follow an item of data as it traverses . It will include diagrams. It will start at the data source, through collect, through curate, and through consumption by users, machine destinations, applications, and so on.

Privacy, Security, and Governance

Privacy

Privacy by Design

Attribute-Based Access Control

User Authorizations

Authorizations are configurable properties assigned to system users. Authorizations are defined by the administrator in accordance with the organization's governance policies. Authorizations are combined with data visibilities to determine what permission a user has to interact with different data. For example, a user with Clinician authorization might be allowed to access all forms of health data, including confidential or identifiable information, while a user with Researcher authorization might be allowed to consume only with de-identified or nonidentified information.

Authorizations are used in access policies together with data visibilities that have been applied to data sources. The access policy matches the authorization against the data visibility to determine what action, if any, a user may take with respect to the data.

Some examples of possible user authorizations are as follows:

- C_LEVEL: The user is a C-Level individual (for example, CEO, COO, CIO, or CTO) with a privileged level of access. Individuals with C_LEVEL authorization, for example, might be permitted to read data with CONFIDENTIAL visibility.
- DOCTOR: A user with DOCTOR authorization might, for example, be permitted to read any information, including personally identifiable information or personal health information.
- ANALYST: A user with ANALYST information might be restricted to accessing de-identified or nonidentified data.

A user can be assigned multiple authorizations. Authorizations are defined as part of system configuration.

Note: Once defined, a user authorization may be neither edited nor deleted.

Data Visibilities

All raw data and derived data stored in the PHEMI system can be tagged with attributes that provide information about the data's sensitivity and the visibility it should have to different system users. These attributes are called data visibilities.

The visibilities you define for your data should reflect the sensitivity of the data as identified by your organization. The PHEMI system predefines three visibilities pertaining to privacy:

Table 1: System-Defined Data Visibilities

Visibility	Description
IDENTIFIED	Sensitive data that contains identifying information. Such data should be secured and available only to authorized personnel.

Visibility	Description
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 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.

Any data visibility defined in the system can be used by a Data Processing Function (DPF) to tag data elements, or cells, derived by the DPF. 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 "cell-level" privacy protection.

Access Policies

An access policy is a set of logical rules that determines how users can consume data stored in the PHEMI system. Access policies can be optionally applied to data sources and datasets.

To create an access policy, you define one or more access rules. In each rule:

- The Subject specifies a set of the user authorizations.
- The Object specifies a set of data visibilities.
- The Action specifies the action to be taken if the rule is matched.

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 access rule within a policy, the rules are related by OR logic.

The rules in a given access policy are intended to implement specific controls over a dataset. 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.

Security

Role-Based Access

Password Policies

Network Security

Audit Log

The Audit Log shows how the PHEMI system has been accessed and used.

The log tracks all accesses to the PHEMI system: through the RESTful API or through the Management Console.

Governance

Governance Policies

To protect your data and the privacy of your data, you should have your organization's governance policy in place before configuring the PHEMI system. A governance policy is a coordinated approach to protecting data and assigning privileges to users.

There are three main aspects to a governance policy:

- Data visibility. Data can have different levels of visibility or sensitivity, and your organization may need to protect different data in different ways. You may want some data visible to every user but other data visible only to selected users. In the PHEMI system, these levels are called "data visibilities." *Tell me more about data visibilities*
- User authorizations. Different users may be required to interact with data differently. For example, clinicians might be allowed to access all data, while researchers might be allowed to read only non-identified or de-identified data. *Tell me more about user authorizations*
- Access policies. Your organization's governance policy will state how users with different authorizations can interact with data of different visibility. *Tell me more about access policies*

The data visibilities, user authorizations, and access policies defined in your governance policies will drive how you configure the PHEMI system. If you are uncertain as to the appropriate data visibilities, user authorizations, or access policies to define for your organization, consult with your Information Officer, Privacy Officer, or with someone in a comparable role.

Data-Sharing Agreements

Lifecycle Management