Privacy, Security, and Governance continued

Build Your Access Policy Quickly and Easily

PHEMI Central tags sensitive data to identify its visibility, captures user authorizations, and combines them in simple, powerful access rules for attribute-based access control.

Role Based Access Control

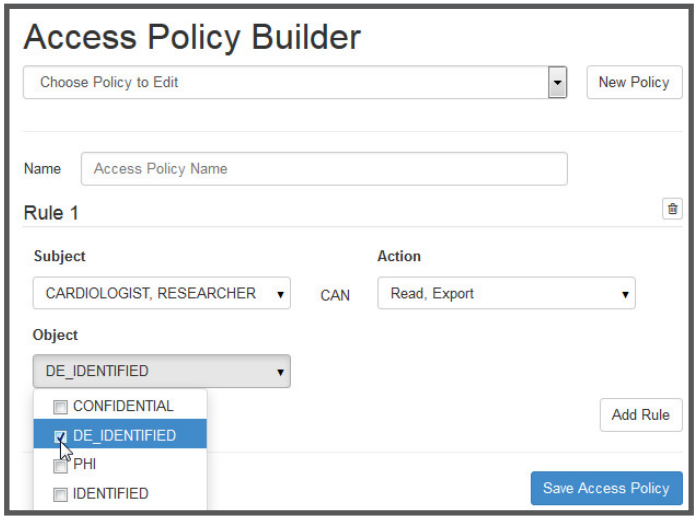
User roles determine what operations a user can perform. For example, only users with a role of administrator can configure the system, while only users with a role of data analyst can execute or export a dataset.

Attribute Based Access Control

Users can be tagged with attributes that describe their level of authorization. Data can be tagged with attributes that describe its level of sensitivity or its requirements for privacy. Together, these two attributes can be combined to allow sophisticated access privileges to identified, unidentifiable, de-identified, or anonymized data.

Audit Log

PHEMI Central maintains complete audit logs of system and user operations. They include all create/modify/delete operations, along with a record of all queries made to the system through the REST interface. These log files are completely tamperproof for all users. Approved users can filter log files and export the information for downstream analysis and compliance reporting.



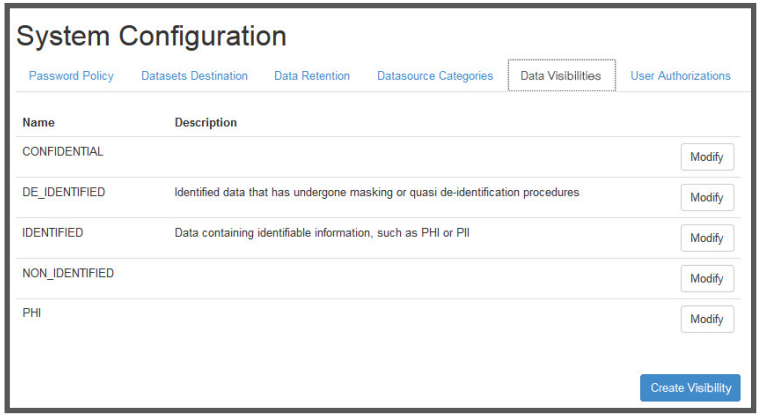
Encryption at Rest

For performance reasons, it is usually unnecessary to encrypt all data. Instead, encryption of only personally identifiable information is advised. PHEMI Central allows you to specify what data must be encrypted when at rest within the system.

Encryption in Motion

PHEMI Central can encrypt links from data sources and to consuming applications and analytics tools using either Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

Define Data Visibilities



Define User Authorizations