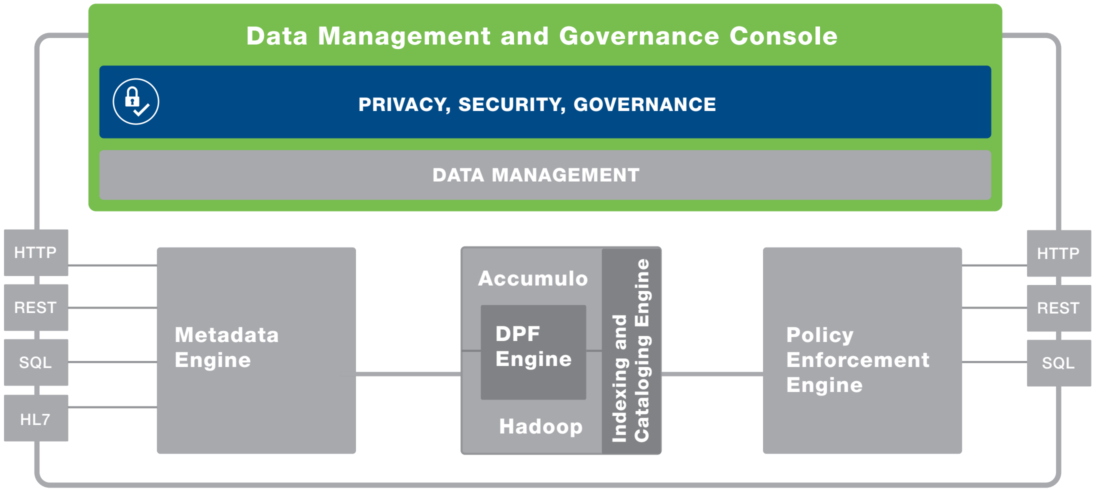
Privacy, Security, and Governance

Protect Sensitive Information at Scale

Information governance is about controlling an organization's data. The data may be sensitive; or perhaps it is important that the data be absolutely accurate; or perhaps the organization must achieve legislative and compliance targets. Data governance includes the process and policies around the protection, curation, and access to data. Data governance encompasses all of privacy protection, data security, and data audit. PHEMI Central helps organizations achieve compliance objectives by providing an industry-pioneering set of capabilities to manage the privacy, security, and governance of data. These capabilities are fully configurable and are automatically enforced throughout the data lifecycle.


Data Management and Governance Console
PRIVACY, SECURITY, GOVERNANCE
DATA MANAGEMENT
HTTP
REST
SQL
HL7
Metadata Engine
Accumulo
DPF Engine
Hadoop
Indexing and Cataloging Engine
Policy Enforcement Engine
HTTP
REST
SQL

Privacy is Built Right Into PHEMI Central Design

Privacy by Design Principles	PHEMI Central Implementation	PHEMI Design Innovation
Proactive, not reactive	Metadata enables policies to define data access	**Data firewalls protect data internally, not just externally** **Rely on automated operational policies, instead of manual processes** **Proper management and control enables positive use of private data**
Privacy as default setting	Assets are immutable. Policies required to access data	
Privacy embedded in design	Metadata and computational access are the core of the system	
Full functionality — positive sum, not zero sum	Data governance policies enable data use/analysis and do not create restrictions	
End-to-end security — full lifecycle protection	Digital assets self-specify how they are managed and handled	
Visibility and transparency — keep it open	Metadata and auditing provide accountability	
Respect for user privacy — keep it user-centric	Data steward defines and sets policies on use	

Privacy by Design

PHEMI Central was built from the ground up on an **innovative Privacy by Design framework** to define, manage, and enforce data sharing agreements and privacy policies. Because PHEMI Central's privacy, security, and governance features are one coordinated design across the system, you don't have to rely on a cobbled-together mish-mash of security mechanisms to protect your organization's sensitive data.

Privacy, Security, and Governance continued

Build Your Access Policy Quickly and Easily

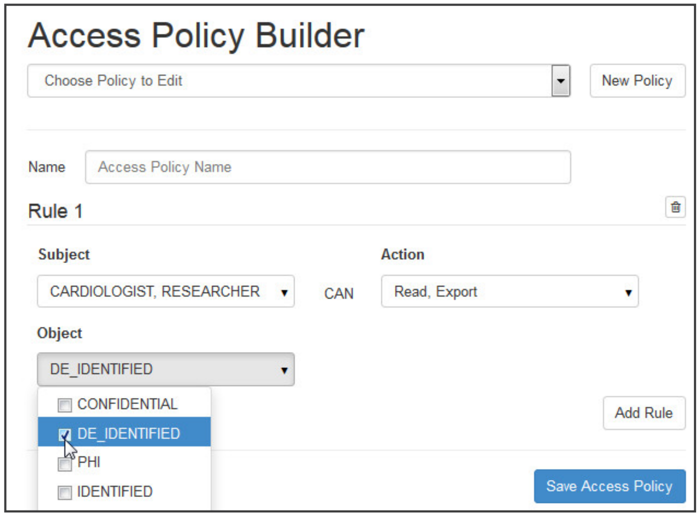
PHEMI Central tags sensitive data to identify its visibility, captures user authorizations, and combines them in simple, powerful access rules for attribute-based access control.

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.



Access Policy Builder

Choose Policy to Edit

Name: Access Policy Name

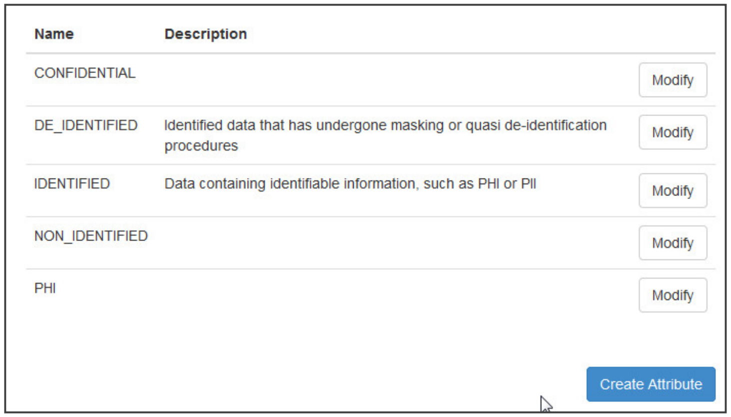
Rule 1

Subject: CARDIOLOGIST, RESEARCHER CAN Action: Read, Export

Object: DE_IDENTIFIED

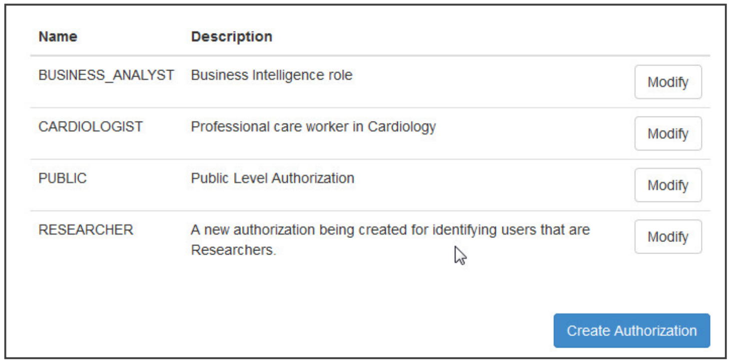
□ CONFIDENTIAL
☑ DE_IDENTIFIED
□ PHI
□ IDENTIFIED

Access Policy Attribute Table



Name	Description	
CONFIDENTIAL		Modify
DE_IDENTIFIED	Identified data that has undergone masking or quasi de-identification procedures	Modify
IDENTIFIED	Data containing identifiable information, such as PHI or PII	Modify
NON_IDENTIFIED		Modify
PHI		Modify

Access Policy Authorization Table



Name	Description	
BUSINESS_ANALYST	Business Intelligence role	Modify
CARDIOLOGIST	Professional care worker in Cardiology	Modify
PUBLIC	Public Level Authorization	Modify
RESEARCHER	A new authorization being created for identifying users that are Researchers.	Modify

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).