

Privacy, Security, and Governance

Contents

Privacy, Security, and Governance.....3

 Privacy.....3

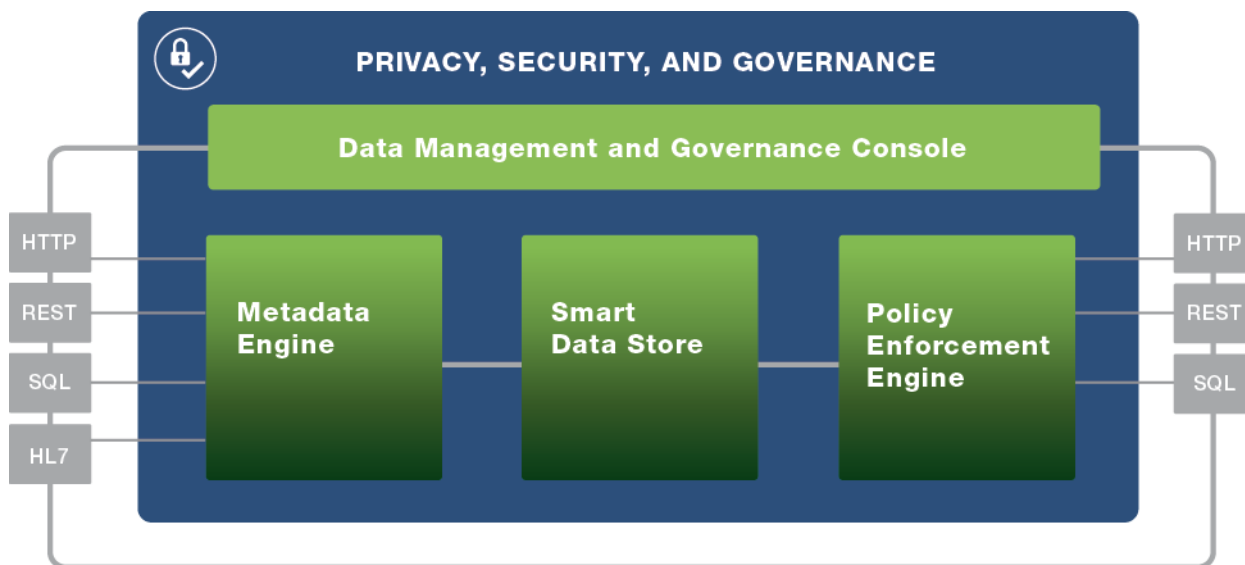
 Security.....4

 Governance.....4

Privacy, Security, and Governance

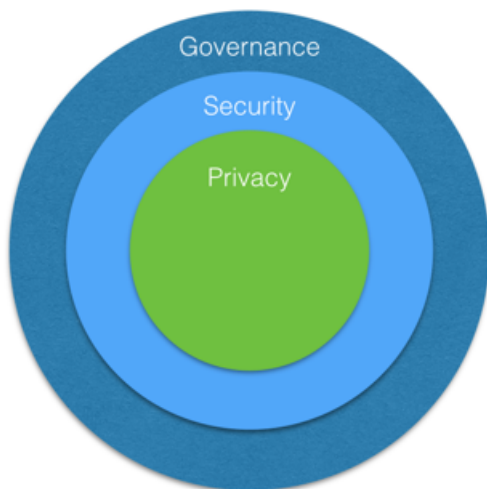
The intention of privacy, security, and governance is to protect information and ensure rightful access.

PHEMI Central is designed from the ground up to be able to manage crucial aspects of privacy and security, and to be able to accurately reflect your organization's governance policies.



Privacy, security, and governance are not all the same thing.

- Privacy is restricting information access to those who have the right to access it.
- Security is the means by which you maintain privacy and protect information assets.
- Governance is the set of processes, roles, policies, controls, and metrics that an organization develops and implements around information to manage its privacy and security.



Privacy

Privacy is restricting information access to those who have the right to access it.

PHEMI Central's Privacy by Design framework was designed from the ground up to define, manage, and enforce data sharing agreements and privacy policies. This framework includes the following mechanisms:

- **Attribute-based access control (ABAC)**—Users are tagged with attributes that describe their authorizations to access data. Data is tagged with attributes that describe what its visibility should be. These two attributes are used in access policies that are applied to data collections and datasets to enforce rightful access privileges. For example, a data analyst with CONFIDENTIAL authorization might be able to export fully identified data, an analyst with RESEARCHER authorization might only have access to de-identified data.

Attribute based access control reduces complexity and reduces the risk of data breach. An attributed-based approach to privacy is also especially helpful when not all uses or access requirements for data are understood up-front, or when new types of data are frequently introduced into the system (both common scenarios in health care, for example).

- **Selective data tagging**—The attribute-based access configured in the system can be enriched and expanded with context-specific protections by using the Data Processing Function framework to extract and re-tag information. For example, scans of patient reports can be recognized and extracted by a DPF and fields selectively marked as PII (personally identifying information, as in a Social Security or Social Insurance Number) or NON_IDENTIFYING (as in a blood glucose measurement).
- **Automatic anonymization and de-identification**—PHEMI Central can be set to automatically invoke a Data Processing Function that can de-identify, encrypt, redact, or mask any data element. A DPF can even include sophisticated data dependency algorithms to reduce the risk of re-identification.

A PHEMI Administrator can also construct datasets that strip out identifying data elements. Centralizing anonymization and de-identification helps reduce data sprawl and reduces the risk of data consistency errors.

- **End to end access policy enforcement**—Every query for data to PHEMI Central is mediated by the PHEMI Policy Enforcement Engine, which compares the access request against the privacy protections that have been placed on the data. At no time can users, applications, or external systems bypass the Policy Enforcement Engine to access data directly.

Security

Security is the means by which you maintain privacy and protect information assets.

PHEMI Central includes a number of security mechanisms:

- **Role Based Access Control (RBAC)**—User roles determine what operations a user can perform. For example, only users with a role of PHEMI Administrator can configure the system and construct datasets, while only users with a role of Data Analyst can query data and execute or export a dataset.
- **Configurable Password Policy**—PHEMI Central allows you to configure the password policy that defines how strong user passwords have to be and how they must be changed.
- **Audit Log**—PHEMI Central maintains complete a audit log of system and user operations. The log includes all create, modify, and delete operations, plus a record of all queries for made to the system. The audit log file is completely tamperproof for all users.
- **Encryption in motion**—PHEMI Central assumes your system is deployed on a trusted network. However, you can encrypt links from data sources and to consuming applications and analytics tools using either Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

Governance

Governance is the set of processes, roles, policies, controls, and metrics that an organization develops and implements around information to manage its security and privacy.

Information governance is about controlling and protecting 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 and encompasses all of privacy protection, data security, lifecycle management, and data audit.

A governance policy is a coordinated approach to protecting data and assigning privileges to users. To control and protect your data, your organization should have a clearly defined policy governing data. The governance policy will drive how the PHEMI Administrator configured PHEMI Central.

How do I define a governance policy?