Privacy by Design at PHEMI

About PHEMI Health Systems

PHEMI™ Health Systems is a process automation and analytics company that unlocks patient data to improve clinic productivity, patient outcomes and medical research.

From organizational practices to product design principles, privacy is at the core of what we do. We bring privacy and security to Big Data to address the unique demands of healthcare. We believe individuals should have control over their personal medical information and that healthcare organizations can simultaneously have access to the type of information they need to provide breakthrough patient care, research and medical innovation.

Based on a framework for effective privacy protection, the PHEMI solution is built upon two complementary platforms:

- **PHEMI Clinical** - a highly customizable care management platform that improves clinic productivity and patient outcomes by automating ambulatory care processes.
- **PHEMI Central** - A fully extensible digital asset library that supports the collection, storage and analysis of a rich dataset of healthcare information for population health management, clinical study engagement, post-market surveillance and curiosity-based research.

Addressing the 7 Foundational Principles of Privacy by Design

Whereas many systems view privacy and security as an afterthought, we architected PHEMI Clinical and PHEMI Central from the ground up specifically for healthcare to fully incorporate the 7 foundational principles of Privacy by Design as applied to Big Data:

1. **Proactive not Reactive; Preventative not Remedial**

PHEMI Central contains a sophisticated Governance Policy Manager that data stewards use to define what data may be stored, how it may be manipulated, and who is allowed to read the data. Permitted personal information can only be collected in the PHEMI system if enabled by the Governance Policy Manager. The data steward creates all policies for user access to the system and datasets. A policy enforcement layer in the PHEMI architecture enforces strict policy rules.

2. **Privacy as the Default Setting**

Data can only be stored in PHEMI Central once the data steward establishes a privacy policy. Furthermore, the system default prevents anyone, other than the data owner, to access the data. The data steward can relax these defaults to allow specific users and roles to access virtual databases within the Big Data repository. We designed the PHEMI solution on the foundation that privacy policies determine what data can be accessed through the de-identification/anonymization processes defined by the Governance Policy Manager. Policies include fine-grained write-only, read-only and read/write permissions.

3. **Privacy Embedded into Design**

As PHEMI Central ingests data, it converts it into a digital asset comprised of the data itself plus metadata – a wrapper that embeds privacy/governance rules, policies and semantics for the digital asset being gathered and stored.
A policy enforcement engine ensures that all users have the appropriate access privileges throughout the Big Data repository. Users can only view digital assets if they have been granted access in a policy established by the data steward using the Governance Policy Manager. Fine-grained policies enforce de-identification of information.

4. Full Functionality - Positive Sum, not Zero Sum

We believe individuals’ privacy rights can co-exist with healthcare organizations’ legitimate medical interests and objectives based on patient consent. PHEMI’s ground-up approach to privacy works symbiotically with clinicians’ needs for complex data analysis. PHEMI’s treatment of data as digital assets means that healthcare data can be enriched and analyzed for meaningful statistics and patterns, with privacy enforcement underpinning the process. No complicated overhead or tradeoff is needed for policy enforcement because users only interact with approved data that has passed through the Governance Policy Manager.

5. End-to-End Security - Full Lifecycle Protection

PHEMI brings lifecycle privacy to Big Data. All digital assets are immutable and only accessible through the PHEMI Governance Policy Manager. Our metadata tagging enables automatic data retention enforcement, access controls and compliance management. For example, if a digital asset has metadata indicating that the asset must be held for ten years, then the data will be automatically deleted on the tenth anniversary. Furthermore, all assets are version controlled so the data steward can review and recover any changes.

Additionally, the audit and logging system in PHEMI Central uses the same digital asset approach to store and manage log files, ensuring that logs are also immutable and only accessible to specific administrative roles.

6. Visibility and Transparency - Keep it Open

PHEMI’s privacy policy implementation is transparent and accessible to data stewards. De-identification and anonymization process rules can also be easily provided to individuals and organizations. PHEMI produces detailed audit logs to verify privacy policy enforcement.

7. Respect for User Privacy - Keep it User-Centric

PHEMI Health Systems recognizes an individual’s paramount right to privacy and our technology core reflects this. With default privacy settings and a sophisticated governance and policy management approach, we ensure an individual’s privacy remains intact. Yet our unique implementation also enables clinicians and researchers access to a rich dataset of healthcare information for pioneer medical innovation and research based on patient consent.

About Privacy by Design (PbD)

Privacy by Design is a framework that was developed by the Information and Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian. Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organization’s default mode of operation. In October 2010, Privacy by Design was recognized as the global privacy standard in a landmark resolution by the International Conference of Data Protection and Privacy Commissioners in Jerusalem.

In October 2013, PHEMI Health Systems was selected as a PbD Ambassador, an exclusive, but growing, group of privacy thought-leaders committed to ensuring the ongoing protection of personal information by following the Principles of PbD. PHEMI is proud to continue advancing the case of embedding privacy protective measures in technology, processes and physical design.