

ASPISMED

FUNCTIONAL & TECHNICAL SPECIFICATIONS: SECURING RWD

DATA PRIVACY & SECURITY FRAMEWORK

Strategic Core Objective:

To safeguard patient integrity and clinical reliability within the ASPISMED ecosystem, we enforce a strict defense-in-depth security model. This architectural framework guarantees that while high-value Real-World Data (RWD) is collected for compliant clinical analytics and pharmaceutical research, individual identities remain mathematically and operationally decoupled from the analytical pipelines.

CORE ARCHITECTURAL PILLARS

1. Source Pseudonymization & De-identification Pipeline

All Personally Identifiable Information (PII) is cryptographically tokenized and pseudonymized at the exact point of origin (source-side) before leaving the client environment. Data ingestion is subsequently routed through an automated, multi-layered de-identification pipeline engineered to minimize residual re-identification risks to the absolute minimum.

2. Privacy-Preserving Computation & Workflow Masking

Advanced privacy-preserving computation techniques isolate identity-sensitive records completely from analytical and AI workflows. Furthermore, clinician patterns and operational data points are secured via workflow masking and granular access controls to shield and safeguard provider-sensitive operational intelligence.

3. Access Control & Immutable Auditing

All administrative, system, and clinical access is governed by strict Role-Based Access Control (RBAC) models, strictly restricting view and modification permissions to authorized personnel only. Every operational interaction is continuously documented via a cryptographically verifiable, append-only immutable audit trail ensuring total accountability.

4. Sovereign Consent & Data Residency

The underlying storage architecture natively enforces strict regional data residency policies and localization. This is paired with a granular, patient-controlled consent protocol, allowing individuals direct authority and sovereign lifecycle management over their shared data assets.

5. Regulatory Compliance & Enterprise Research Readiness

By natively intertwining these paradigms, the ASPISMED architecture establishes absolute compliance with major global regulatory standards, including **GDPR** and **HIPAA**. The resulting data outputs provide premium-tier, risk-reduced, anonymized datasets fully optimized for compliant pharmaceutical research and next-generation clinical analytics.