Product Requirements Document

Organizational Ontology Integration for Privacy Firewall

Version: 1.0
Date: September 2025
Author: Lawrence Lu
Stakeholder: LLM Security Team, working with the LLM Data team

---

Executive Summary

Integrate the AI Privacy Firewall with the organization's semantic ontology to enable context-aware privacy decisions based on a deep understanding of business concepts, data relationships, and domain-specific rules, reducing privacy errors by 85%.

Problem Statement

Current privacy rules operate on surface-level pattern matching without understanding semantic meaning, causing:

- **Context blindness**: "Revenue" in sales vs. HR contexts treated identically
- **Relationship ignorance**: Cannot infer that "compensation" includes "salary," "bonus," "equity."
- **Domain confusion**: Medical "diagnosis" vs. IT "diagnosis" filtered incorrectly
- **Rule explosion**: manual rules to cover concept variations

Solution Overview

Leverage the enterprise RDF/OWL ontology to provide semantic reasoning capabilities:

```
# Example ontology relationships
:SensitiveData rdfs:subClassOf :Data .
:MedicalRecord rdfs:subClassOf :SensitiveData .
:Diagnosis rdfs:subClassOf :MedicalRecord .
:PatientDiagnosis owl:equivalentClass :Diagnosis .

:hasAccessTo rdfs:domain :Role ;
        rdfs:range :DataClass ;
        owl:TransitiveProperty .
```

:Doctor :hasAccessTo :MedicalRecord .
:MedicalRecord :includes :Diagnosis .
Therefore: Doctor hasAccessTo Diagnosis (inferred)

Key Capabilities

Capability	Current State	With Ontology
Concept Recognition	Exact string matching	Semantic understanding with synonyms, hierarchies
Relationship Inference	Explicit rules only	Transitive, symmetric, inverse reasoning
Context Disambiguation	Manual context rules	Domain-aware classification
Compliance Mapping	Hard-coded regulations	Semantic compliance rules

Core Ontology Requirements

Essential Concepts

Data Classifications:
- PublicData
- InternalData
- ConfidentialData
- RestrictedData
  - PersonalData (PII)
  - HealthData (PHI)
  - FinancialData (PCI)

Organizational Contexts:
- HealthcareDomain
  - ClinicalContext
  - BillingContext
  - ResearchContext
- FinancialDomain
  - TradingContext
  - AccountingContext

Information Relationships:
- contains (transitive)

- derivedFrom (tracks lineage)
- semanticallyEquivalent
- requiresConsentFor

Reasoning Rules

```
# Rule: Information derived from sensitive data inherits sensitivity
CONSTRUCT {
  ?derived rdf:type :SensitiveData
}
WHERE {
  ?derived :derivedFrom ?source .
  ?source rdf:type :SensitiveData .
}

# Rule: Aggregate data from 3+ individuals is less sensitive
CONSTRUCT {
  ?data :sensitivityLevel "low"
}
WHERE {
  ?data :aggregationCount ?count .
  FILTER(?count >= 3)
}
```

Use Case Examples

Use Case 1: Hierarchical Data Understanding

- **Input**: "Show patient's test results"
- **Ontology**: `TestResult ⊆ MedicalRecord ⊆ PHI`
- **Decision**: Apply PHI protection rules automatically

Use Case 2: Cross-Domain Disambiguation

- **Input**: "Customer profile data"
- **Ontology Context**: In FinancialDomain vs. HealthcareDomain
- **Decision**: Different filtering based on domain-specific regulations

Use Case 3: Equivalent Concept Recognition

- **Input**: Various terms: "SSN", "Social Security Number", "TIN"
- **Ontology**: All map to `TaxIdentificationNumber`
- **Decision**: Consistent filtering regardless of terminology