MedShare Hub

Healthcare Data Exchange Platform

Product Requirements Document (PRD)

Version:	1.0
Date:	January 30, 2026
Status:	Draft
Author:	Product Team

Table of Contents

1. Executive Summary

MedShare Hub is a next-generation healthcare data exchange platform designed to enable secure, compliant, and granular sharing of medical records across hospitals, clinics, insurance providers, research institutions, and patients. Built on Attribute-Based Access Control (ABAC) architecture, the platform ensures HIPAA compliance while providing unprecedented flexibility in access management.

The platform addresses critical gaps in existing healthcare information systems by moving beyond traditional role-based access control to support context-aware, policy-driven authorization that respects patient consent, emergency scenarios, data sensitivity, and regulatory requirements.

Key Highlights

- Multi-tenant architecture supporting 1000+ healthcare organizations
- Sub-100ms policy evaluation for real-time access decisions
- Full HIPAA and GDPR compliance with comprehensive audit trails
- Support for emergency break-glass access with enhanced logging
- Patient-controlled consent management and data sharing preferences

2. Product Overview

2.1 Vision

To become the trusted backbone of healthcare data exchange, enabling seamless, secure, and patient-centric sharing of medical information while maintaining the highest standards of privacy and regulatory compliance.

2.2 Mission

Empower healthcare providers, patients, insurers, and researchers with intelligent access control that balances security, usability, and compliance through advanced ABAC technology.

2.3 Target Market

Segment	Description	Priority
Hospital Networks	Multi-facility healthcare systems (50-500 beds)	Primary
Insurance Providers	Health insurance companies and payers	Primary
Ambulatory Clinics	Outpatient care facilities and specialist clinics	Secondary
Research Institutions	Academic medical centers and clinical trial organizations	Secondary
Individual Patients	Patient portals for personal health record management	Tertiary

3. Problem Statement

3.1 Current Challenges

• **Inflexible Access Control:** Traditional role-based access control (RBAC) cannot handle the complexity of healthcare scenarios where access depends on patient consent, treatment relationships, data sensitivity, time constraints, and emergency situations.

• **Compliance Burden:** Healthcare organizations struggle to maintain HIPAA compliance while enabling necessary data sharing. Manual audit processes are time-consuming and error-prone.

• **Patient Empowerment Gap:** Patients have limited control over who accesses their medical records and for what purposes, leading to privacy concerns and reduced trust.

• **Interoperability Issues:** Disparate systems across healthcare organizations make it difficult to share data securely while maintaining proper access controls.

• **Emergency Access Dilemma:** During medical emergencies, providers need immediate access to patient records, but current systems either block access entirely or provide overly broad permissions.

3.2 Market Opportunity

The global healthcare information exchange market is projected to reach $2.4 billion by 2027, growing at 9.2% CAGR. With increasing regulatory scrutiny and patient data breaches costing healthcare organizations an average of $10.1 million per incident, there is urgent demand for advanced access control solutions.

4. User Personas

Dr. Sarah Chen - Cardiologist

Role: Treating Physician

Goals:

• Quick access to patient cardiac history during consultations

• View treatment timeline and medication interactions

• Securely share findings with referring physicians

Pain Points:

• Multiple logins across different hospital systems

• Cannot access records when patient transfers from another facility

• Unclear what data patients have consented to share

James Rodriguez - Insurance Claims Adjuster

Role: Claims Processor

Goals:

• Access billing codes and treatment justification

• Verify medical necessity for procedures

• Process claims efficiently without violating patient privacy

Pain Points:

• Sees more patient data than necessary for claims

• Manual redaction of sensitive information

• Audit trail requirements slow down processing

Maria Thompson - Patient

Role: Healthcare Consumer

Goals:

• Control who can see my medical records

• Grant temporary access to family members

• Understand how my data is being used

Pain Points:

• No visibility into who accessed my records

• Cannot easily share records with new specialists

• Concerns about data privacy and security

Dr. Michael Park - Emergency Physician

Role: Emergency Department Physician

Goals:

• Immediate access to critical patient information

• View allergy information and current medications

• Make informed decisions during life-threatening situations

Pain Points:

• Delayed access to records during emergencies

• Unknown patient medical history

• Risk of adverse drug interactions

5. Functional Requirements

Authentication & Authorization

FR-1.1: Support SSO integration with hospital identity providers (SAML, OAuth2, OIDC)

FR-1.2: Multi-factor authentication for all user types

FR-1.3: Real-time policy evaluation (sub-100ms response time)

FR-1.4: Dynamic attribute resolution from multiple sources

Data Access & Sharing

FR-2.1: Support FHIR R4 and HL7 v2 standards for medical data exchange

FR-2.2: Granular data filtering based on field-level sensitivity

FR-2.3: Automatic data redaction for unauthorized fields

FR-2.4: Support for structured and unstructured medical documents

Patient Consent Management

FR-3.1: Patient portal for managing consent preferences

FR-3.2: Granular consent controls by data type, provider, and purpose

FR-3.3: Temporary access delegation to family members/caregivers

FR-3.4: Consent expiration and automatic revocation

Emergency Access

FR-4.1: Break-glass mechanism for emergency override

FR-4.2: Mandatory justification for emergency access

FR-4.3: Real-time supervisor notification

FR-4.4: Enhanced audit logging for emergency access events

Audit & Compliance

FR-5.1: Comprehensive audit trail of all access events

FR-5.2: Tamper-proof audit logs with cryptographic signatures

FR-5.3: Real-time anomaly detection and alerting

FR-5.4: Automated compliance reporting (HIPAA, GDPR)

6. ABAC Access Control Requirements

6.1 Attribute Categories

Category	Examples	Source
Subject Attributes	Role, Department, Certifications, Employer, Locatio	Identity Provider, HR System
Resource Attributes	Data Type, Sensitivity Level, Patient ID, Creation Date	Medical Records System
Action Attributes	Read, Write, Update, Delete, Export, Print	Application Context
Environment Attributes	Time, Day of Week, IP Address, Device Type, Network	Runtime Context
Relationship Attributes	Treating Physician, Consulting Specialist, Care Team Member	EHR System

6.2 Policy Examples

Policy 1 - Treating Physician Access: A physician can read medical records IF they have an active treatment relationship with the patient AND the access occurs during business hours (8AM-8PM) AND the data sensitivity level is not 'psychiatric' (unless the physician is in the psychiatry department).

Policy 2 - Insurance Claims: A claims adjuster can read billing codes and diagnosis information IF they have an active claim assigned for that patient AND the patient has consented to insurance data sharing AND they CANNOT access clinical notes or sensitive diagnoses.

Policy 3 - Patient Access: A patient can read ALL their own records at any time with no restrictions, AND can grant temporary read access to designated family members with expiration dates.

Policy 4 - Emergency Override: An emergency-certified physician can access critical patient information during declared emergencies regardless of other restrictions, but MUST provide justification AND triggers supervisor notification AND creates enhanced audit log entry.

7. Non-Functional Requirements

ID	Category	Requirement	Target
NFR-1	Performance	Policy evaluation latency	< 100ms (p95)
NFR-2	Performance	API response time	< 500ms (p95)
NFR-3	Scalability	Concurrent users	100,000+
NFR-4	Scalability	Policy evaluations per second	10,000+
NFR-5	Availability	System uptime	99.9%
NFR-6	Security	Data encryption	AES-256 at rest, TLS 1.3 in transit
NFR-7	Security	Failed authentication rate	< 0.1%
NFR-8	Compliance	HIPAA compliance	100% adherence
NFR-9	Compliance	Audit log retention	7 years minimum
NFR-10	Usability	User onboarding time	< 15 minutes
NFR-11	Reliability	Data loss tolerance	Zero data loss (RPO = 0)
NFR-12	Reliability	Recovery time objective	< 4 hours

8. User Stories

US-1: High Priority

As a **Cardiologist**, I want **to view cardiac test results for my patients** so that **I can make informed treatment decisions**.

Acceptance Criteria:

• Can access cardiac records within 2 seconds

• Only see records for patients under my active care

• Cannot access psychiatric or sensitive notes

• All access is logged for audit purposes

US-2: High Priority

As a **Patient**, I want **to control who can access my medical records** so that **I can maintain privacy and trust in the healthcare system**.

Acceptance Criteria:

• Can view list of all providers with access

• Can revoke access at any time

• Can set expiration dates for temporary access

• Receive notifications when records are accessed

US-3: Medium Priority

As a **Insurance Claims Processor**, I want **to access only billing-relevant information** so that **I can process claims without violating patient privacy**.

Acceptance Criteria:

• Can view diagnosis codes and procedure codes

• Cannot access clinical notes or sensitive diagnoses

• Data is automatically redacted based on claim type

• Access is limited to assigned claims only

US-4: Critical Priority

As a **Emergency Physician**, I want **to access critical patient information during emergencies** so that **I can provide life-saving treatment**.

Acceptance Criteria:

• Can override normal restrictions during declared emergencies

• Must provide justification for emergency access

• Supervisor is notified in real-time

• Enhanced audit log is created

• Access expires after emergency period ends

US-5: High Priority

As a **Compliance Officer**, I want **to generate audit reports showing all access patterns** so that **I can ensure HIPAA compliance and investigate breaches**.

Acceptance Criteria:

• Can filter audit logs by user, patient, date range, action

• Reports show all failed and successful access attempts

• Can identify unusual access patterns

• Export reports in multiple formats (PDF, CSV, Excel)

9. Success Metrics

Metric	Target	Measurement Method
User Adoption Rate	80% within 6 months	Active users / Total licensed users
Policy Evaluation Performance	< 100ms (p95)	APM monitoring
Audit Compliance Score	100%	Automated compliance scans
Patient Satisfaction (NPS)	> 40	Quarterly patient surveys
Provider Satisfaction	> 4.0/5.0	Monthly provider feedback
System Uptime	99.9%	Infrastructure monitoring
Security Incident Rate	< 1 per quarter	Security incident tracking
Emergency Access Time	< 30 seconds	Performance logs
False Positive Rate (Access Denials)	< 2%	Support ticket analysis
Consent Management Usage	> 60% of patients	Portal analytics

9.1 Business Impact Metrics

• Reduce average data breach cost by 60% through granular access control

• Decrease compliance audit preparation time by 75%

• Improve patient trust scores by 30%

• Reduce help desk tickets related to access issues by 50%

• Increase data sharing efficiency between organizations by 40%

10. Risks and Mitigations

Risk	Impact	Probability	Mitigation Strategy
Policy complexity leads to performance degradation	High	Medium	Implement policy optimization tools, caching, and regular performance testing
Legacy system integration challenges	High	High	Build robust API adapters, provide extensive documentation, phased rollout
User resistance to new access controls	Medium	Medium	Comprehensive training program, gradual feature rollout, dedicated support
Regulatory compliance gaps	Critical	Low	Engage legal counsel early, regular compliance audits, certifications
Policy authoring errors	High	Medium	Policy simulation tools, peer review process, automated testing
Emergency access abuse	High	Low	Real-time monitoring, supervisor alerts, quarterly audits, strict penalties
Attribute data synchronization delays	Medium	Medium	Real-time event streaming, cache invalidation, fallback mechanisms

Conclusion

MedShare Hub represents a significant advancement in healthcare data exchange technology. By leveraging Attribute-Based Access Control, the platform addresses critical gaps in current systems while maintaining the flexibility to adapt to evolving healthcare needs and regulatory requirements.

The success of this platform will be measured not only by technical metrics but also by its impact on patient safety, provider efficiency, and overall trust in healthcare data systems. With careful planning, robust implementation, and continuous stakeholder engagement, MedShare Hub is positioned to become the industry standard for secure healthcare data exchange.