Product Requirements Document (PRD)

AI-Powered Health Insurance Claim Portal with Fraud Detection

Version: 1.0
Date: November 21, 2025
Document Owner: Product Team
Classification: Internal

---

1. Executive Summary

1.1 Purpose

This document outlines the requirements for developing an automated health insurance claim portal that streamlines the claim submission process while leveraging AI to detect fraudulent activities. The portal will reduce claim processing time by up to 40%, improve accuracy by 80%, and enhance customer satisfaction through a seamless digital experience[1][2].

1.2 Business Objectives

- **Reduce claim processing costs by 30%** through automation[2]
- **Decrease fraudulent claim payouts by 15-20%** using AI-powered fraud detection[3][4]
- **Improve claim turnaround time** from weeks to 24-48 hours for standard claims
- **Enhance customer experience** with 24/7 self-service capabilities
- **Ensure regulatory compliance** with HIPAA, data privacy laws, and insurance regulations[5]

1.3 Target Users

- **Primary:** Policyholders filing health insurance claims
- **Secondary:** Claims adjusters, fraud investigators, customer support agents
- **Tertiary:** System administrators, compliance officers

---

2. Product Overview

2.1 Product Vision

A fully automated, intelligent health insurance claim portal that guides users through a personalized claim journey while using AI to validate information, detect fraud patterns, and expedite legitimate claims processing.

2.2 Key Features

1. **Secure Personalized Entry Links** – Unique, time-bound claim access URLs
2. **Automated Policy Validation** – Real-time policy verification and coverage checks
3. **Intelligent Document Upload** – OCR-powered document extraction and validation[6][7]
4. **AI Conversational Interview** – Dynamic questioning to assess claim legitimacy[8][9]
5. **Fraud Detection Engine** – Multi-layered AI analysis for anomaly detection[3][4]
6. **Real-Time Claim Tracking** – Status updates and notifications
7. **Admin Dashboard** – Claims review, approval workflow, and fraud alerts

2.3 Success Metrics

Metric	Current State	Target (6 months)
Average Processing Time	14-21 days	1-2 days
Claim Denial Rate	32%	<15%
Fraud Detection Rate	60%	85%+
False Positive Rate	30%	<10%
Customer Satisfaction (CSAT)	3.2/5	4.5/5
Cost per Claim Processed	$80	$50

---

3. User Journeys & Workflows

3.1 Primary User Flow: Claimant Journey

Phase 1: Entry & Authentication

1. **Claim Link Generation**
   - System generates unique, tokenized URL with 7-day expiry
   - Link sent via email/SMS with claim reference number
   - Contains encrypted policy holder ID and claim type parameters
2. **Secure Portal Access**
   - User clicks personalized link
   - System validates token authenticity and expiry
   - Single sign-on (SSO) or one-time password (OTP) verification
   - Session established with 30-minute idle timeout

Phase 2: Policy Validation

1. **Policy Number Entry**
   - User enters policy number or auto-populated from link
   - Real-time validation against policy database
   - System fetches:
     - Policy holder details (name, DOB, coverage type)

        - Active coverage status and benefit limits
        - Deductibles, co-pays, and prior claims history
2. **Coverage Verification**
    - Display applicable coverage for claim type
    - Show remaining benefit limits for the year
    - Alert user of any coverage exclusions
    - Calculate estimated eligible reimbursement

Phase 3: Document Submission

1. **Document Upload Interface**
    - Drag-and-drop or file browser selection
    - Support formats: PDF, JPG, PNG, HEIC (max 10MB per file)
    - Required documents checklist based on claim type:
        - **Hospitalization:** Admission/discharge summary, bills, prescriptions, diagnostic reports
        - **Outpatient:** Doctor consultation receipts, pharmacy bills, prescriptions
        - **Diagnostic:** Lab reports, imaging results, referral letters
2. **OCR Processing & Validation**[6][7]
    - Automated text extraction from uploaded documents
    - Key data points captured:
        - Patient name, provider name, service dates
        - Diagnosis codes (ICD-10), procedure codes (CPT)
        - Bill amounts, payment methods, invoice numbers
    - Real-time validation:
        - Cross-check extracted name vs. policy holder
        - Verify service dates within policy coverage period
        - Validate provider credentials and network status
    - Flag discrepancies for user correction

Phase 4: AI Conversational Interview[8][9]

1. **Context-Aware Questioning**
    - AI analyzes uploaded documents and generates personalized questions
    - Dynamic follow-up based on previous responses
    - Natural language processing for understanding user input
2. **Sample Question Flow (Hospitalization Claim)**
   AI: "I see you were hospitalized from March 10-15. Can you describe the symptoms that led to your admission?"
   User: "Severe chest pain and shortness of breath"
   AI: "When did these symptoms first start?"
   User: "Around 2 days before admission"
   AI: "Did you seek any medical consultation before hospitalization?"
   User: "Yes, visited local clinic on March 9"
   AI: "I notice the hospital bill doesn't show that clinic visit. Do you have receipts from that consultation?"
3. **Fraud Detection Triggers During Interview**[3][4]
    - Inconsistent timeline compared to medical records
    - Vague or overly rehearsed responses
    - Discrepancies between verbal account and documents
    - Unusual claim patterns (e.g., claim submitted shortly after policy purchase)
    - Prior fraud history flags in database

Phase 5: Submission & Processing

1. **Claim Summary Review**
    - Display extracted data and interview responses
    - Allow user to edit/correct information
    - Show estimated processing timeline (1-5 business days)
2. **Submission Confirmation**
    - Generate claim reference ID
    - Send confirmation email/SMS with claim details
    - Provide link for real-time status tracking

3.2 Secondary User Flow: Admin/Adjuster Review

Claim Prioritization

- **Green (Auto-Approve):** Low-risk, within limits, all validations passed
- **Yellow (Review Required):** Minor discrepancies, moderate risk score
- **Red (High Risk):** Fraud flags triggered, requires investigation

Admin Dashboard Features

1. **Claims Queue Management**
    - Sortable by priority, claim amount, submission date
    - Bulk actions (approve, reject, request info)
    - SLA tracking and overdue alerts
2. **Fraud Investigation Tools**
    - Side-by-side document comparison
    - Interview transcript with AI risk annotations
    - Historical claims pattern analysis
    - Network graph showing related claims/providers
3. **Approval Workflow**
    - Multi-level approval for high-value claims (>$10,000)
    - Audit trail of all actions and decisions
    - Direct communication channel with claimant

---

4. Technical Requirements

4.1 System Architecture

Frontend Stack

- **Framework:** Next.js 14+ (React) with TypeScript
- **UI Library:** Tailwind CSS + Shadcn/UI components
- **State Management:** Zustand or React Context
- **Form Handling:** React Hook Form with Zod validation
- **File Upload:** React Dropzone with chunked uploads

Backend Stack

- **API Server:** Node.js with Express or Fastify
- **Authentication:** JWT with refresh tokens, OAuth2.0
- **Database:** PostgreSQL (relational data) + Redis (caching)
- **File Storage:** AWS S3 or Azure Blob Storage with CDN
- **Queue System:** RabbitMQ or AWS SQS for async processing

AI/ML Services

- **Conversational AI:** OpenAI GPT-4 API or Azure OpenAI Service
- **OCR Engine:**
  - Tesseract OCR (open-source baseline)
  - Commercial: Azure Document Intelligence or AWS Textract[6][7]
- **Fraud Detection:**
  - Custom ML model (Python + TensorFlow/PyTorch)
  - Pre-trained: Azure Fraud Detector or AWS Fraud Detector[3][4]
- **NLP Analysis:** SpaCy or Hugging Face Transformers for sentiment/inconsistency detection

Infrastructure

- **Hosting:** AWS/Azure/GCP (multi-region for 99.9% uptime)
- **CI/CD:** GitHub Actions or GitLab CI
- **Monitoring:** Datadog, New Relic, or Prometheus + Grafana
- **Logging:** ELK Stack (Elasticsearch, Logstash, Kibana)

4.2 Database Schema (Core Entities)

Users Table

```
CREATE TABLE users (
user_id UUID PRIMARY KEY,
email VARCHAR(255) UNIQUE NOT NULL,
phone VARCHAR(20),
full_name VARCHAR(255),
date_of_birth DATE,
created_at TIMESTAMP DEFAULT NOW(),
last_login TIMESTAMP
);
```

Policies Table

```
CREATE TABLE policies (
policy_id UUID PRIMARY KEY,
user_id UUID REFERENCES users(user_id),
policy_number VARCHAR(50) UNIQUE NOT NULL,
policy_type VARCHAR(50), -- individual, family, corporate
coverage_amount DECIMAL(12,2),
start_date DATE,
end_date DATE,
status VARCHAR(20), -- active, expired, cancelled
deductible DECIMAL(10,2),
```

```
created_at TIMESTAMP DEFAULT NOW()
);
```

Claims Table

```
CREATE TABLE claims (
claim_id UUID PRIMARY KEY,
policy_id UUID REFERENCES policies(policy_id),
user_id UUID REFERENCES users(user_id),
claim_number VARCHAR(50) UNIQUE NOT NULL,
claim_type VARCHAR(50), -- hospitalization, outpatient, diagnostic
claim_amount DECIMAL(12,2),
claim_date DATE,
submission_date TIMESTAMP DEFAULT NOW(),
status VARCHAR(30), -- submitted, under_review, approved, rejected, pending_info
fraud_risk_score DECIMAL(5,2), -- 0-100 scale
processing_notes TEXT,
approved_amount DECIMAL(12,2),
approval_date TIMESTAMP,
rejection_reason TEXT
);
```

Claim Documents Table

```
CREATE TABLE claim_documents (
document_id UUID PRIMARY KEY,
claim_id UUID REFERENCES claims(claim_id),
document_type VARCHAR(50), -- bill, prescription, report, identity_proof
file_name VARCHAR(255),
file_path TEXT, -- S3 URL
file_size INTEGER, -- in bytes
upload_date TIMESTAMP DEFAULT NOW(),
ocr_extracted_data JSONB, -- structured OCR output
validation_status VARCHAR(20) -- pending, validated, rejected
);
```

AI Interview Table

```
CREATE TABLE ai_interviews (
interview_id UUID PRIMARY KEY,
claim_id UUID REFERENCES claims(claim_id),
question_sequence INTEGER,
question_text TEXT,
user_response TEXT,
response_timestamp TIMESTAMP,
fraud_indicators JSONB, -- detected red flags
sentiment_score DECIMAL(3,2), -- -1 to 1
consistency_score DECIMAL(3,2) -- 0 to 1
);
```

Fraud Flags Table

```
CREATE TABLE fraud_flags (
flag_id UUID PRIMARY KEY,
claim_id UUID REFERENCES claims(claim_id),
flag_type VARCHAR(50), -- document_mismatch, timeline_inconsistency, duplicate_claim
severity VARCHAR(20), -- low, medium, high, critical
description TEXT,
detected_at TIMESTAMP DEFAULT NOW(),
resolved BOOLEAN DEFAULT FALSE,
resolution_notes TEXT
);
```

4.3 API Endpoints

Authentication & Access

```
POST /api/auth/generate-claim-link
POST /api/auth/verify-token
POST /api/auth/refresh-token
```

Claim Submission

```
GET /api/policies/{policyNumber}/validate
POST /api/claims/initiate
POST /api/claims/{claimId}/documents/upload
GET /api/claims/{claimId}/documents
POST /api/claims/{claimId}/interview/start
POST /api/claims/{claimId}/interview/respond
POST /api/claims/{claimId}/submit
GET /api/claims/{claimId}/status
```

Admin/Review

```
GET /api/admin/claims?status={status}&priority={priority}
PUT /api/admin/claims/{claimId}/approve
PUT /api/admin/claims/{claimId}/reject
GET /api/admin/claims/{claimId}/fraud-analysis
POST /api/admin/claims/{claimId}/request-info
```

Analytics

```
GET /api/analytics/claims-summary
GET /api/analytics/fraud-statistics
GET /api/analytics/processing-metrics
```

4.4 Security & Compliance

HIPAA Compliance Requirements[5]

1. **Administrative Safeguards**
    - Designate Privacy Officer and Security Officer
    - Implement workforce training program
    - Establish incident response procedures
    - Regular risk assessments (quarterly)
2. **Physical Safeguards**
    - Secure data centers with access controls
    - Workstation security policies
    - Device and media controls
3. **Technical Safeguards**
    - **Access Control:** Role-based access (RBAC), unique user IDs, automatic logoff
    - **Audit Controls:** Comprehensive logging of all PHI access
    - **Integrity Controls:** Checksums for data transmission
    - **Transmission Security:** TLS 1.3 for all communications
4. **PHI Protection Measures**
    - AES-256 encryption at rest
    - End-to-end encryption for file uploads
    - Data minimization (only collect necessary information)
    - Automatic data anonymization after claim closure (retain 7 years per regulations)
    - Secure document disposal procedures

Additional Security Features

- **Multi-Factor Authentication (MFA):** Required for admin access
- **Rate Limiting:** Prevent brute force and DDoS attacks
- **Input Sanitization:** Prevent SQL injection, XSS attacks
- **API Security:** OAuth 2.0, API key rotation, request signing
- **Penetration Testing:** Quarterly security audits
- **Breach Notification Protocol:** Automated alerts within 72 hours

4.5 AI/ML Model Specifications

Fraud Detection Model Architecture[3][4]

1. **Input Features (60+ parameters)**
    - **Document Analysis:**
        - OCR confidence scores
        - Document authenticity indicators (metadata, fonts, resolution)
        - Duplicate document hash matching across claims database
    - **Claim Characteristics:**
        - Claim amount vs. policy average
        - Time between policy issuance and claim (new policy flag)
        - Claim frequency (multiple claims in short period)
        - Diagnosis-treatment consistency scoring
    - **Provider Analysis:**
        - Provider's historical fraud rate
        - Provider network status
        - Geographic location risk score
    - **Behavioral Indicators:**

        - Interview response coherence score
        - Sentiment analysis (hesitation, defensiveness)
        - Response time patterns
        - Device fingerprinting (same device for multiple claims)
2. **Model Types (Ensemble Approach)**
    - **Random Forest:** Pattern recognition for known fraud types
    - **XGBoost:** High-accuracy classification with feature importance
    - **Neural Network:** Deep learning for complex fraud schemes
    - **Anomaly Detection (Isolation Forest):** Identify outlier claims
3. **Training & Validation**
    - Training dataset: 100,000+ historical claims (60% legitimate, 40% fraudulent)
    - Cross-validation: 5-fold stratified sampling
    - Performance targets:
        - Precision: >85% (minimize false positives)
        - Recall: >90% (catch actual fraud)
        - F1-Score: >87%
        - AUC-ROC: >0.92
4. **Real-Time Scoring**
    - Inference latency: <500ms per claim
    - Risk score output: 0-100 scale
        - 0-30: Low risk (auto-approve eligible)
        - 31-60: Medium risk (review required)
        - 61-85: High risk (detailed investigation)
        - 86-100: Critical risk (flag for fraud unit)

Conversational AI Configuration[8][9]

1. **Language Model:** GPT-4 Turbo or equivalent (128k context)
2. **System Prompt Engineering:**
   You are a health insurance claims assistant. Your goal is to:
    1. Gather accurate information about the claim event
    2. Detect inconsistencies between user responses and uploaded documents
    3. Ask clarifying questions in a friendly, empathetic manner
    4. Flag suspicious patterns without being accusatory

   Document context: {ocr_extracted_data}
   Policy details: {policy_coverage_info}
3. **Question Generation Strategy:**
    - Start with open-ended questions about the incident
    - Progress to specific timeline and detail verification
    - Cross-reference responses with document dates/amounts
    - Use conditional branching based on claim type
4. **Response Analysis:**
    - Sentiment detection (detect anxiety, defensiveness, evasiveness)
    - Consistency scoring (compare responses to documents)
    - Red flag keywords (coached responses, vague details)
    - Response latency analysis (unusually fast or delayed answers)
5. **Safety & Ethics:**
    - No discriminatory questioning based on demographics
    - Clear user consent before AI interview begins
    - Option to speak with human agent at any time
    - Transparent explanation of AI's role in process

5. Non-Functional Requirements

5.1 Performance

- **Page Load Time:** <2 seconds for 90th percentile
- **API Response Time:** <300ms for 95% of requests
- **File Upload Speed:** Support up to 100MB uploads with progress indicator
- **Concurrent Users:** Support 10,000 simultaneous active sessions
- **Database Query Time:** <100ms for policy lookups

5.2 Scalability

- Horizontal scaling for API servers (auto-scaling based on load)
- Database read replicas for query performance
- CDN for static assets and document delivery
- Queue-based processing for AI tasks (async)
- Microservices architecture for independent scaling

5.3 Reliability & Availability

- **Uptime SLA:** 99.9% (max 8.76 hours downtime/year)
- **Disaster Recovery:** Recovery Time Objective (RTO) of 4 hours
- **Backup Strategy:**
  - Daily automated backups with 30-day retention
  - Point-in-time recovery for database
  - Cross-region replication for critical data
- **Failover:** Automatic failover to secondary region

5.4 Usability

- **Accessibility:** WCAG 2.1 Level AA compliance
- **Mobile Responsiveness:** Fully functional on iOS/Android devices
- **Browser Support:** Chrome, Firefox, Safari, Edge (latest 2 versions)
- **Multi-Language:** Support for English, Spanish, Hindi (expandable)
- **Help System:** Contextual tooltips, video tutorials, live chat support

5.5 Monitoring & Observability

- Real-time dashboard for system health metrics
- Automated alerting for:
  - API error rate >5%
  - Response time degradation
  - Fraud detection model failures
  - Security anomalies (unusual login patterns)
- User session recording (with privacy controls)
- A/B testing framework for UI improvements

---

6. Fraud Detection Use Cases

6.1 Scenario 1: Document Manipulation Detection

Trigger: User uploads hospital bill with edited amounts

Detection Mechanism:

- OCR confidence score drops on bill amount field
- Metadata analysis shows file modification timestamp after service date
- Image forensics detect copy-paste artifacts
- Cross-reference with hospital billing system API (if integrated)

System Response:

- Flag claim as "High Risk"
- Request original documents from hospital directly
- Notify fraud investigation team
- Place claim on hold pending verification

6.2 Scenario 2: Timeline Inconsistency

Trigger: Interview reveals discrepancies in event sequence

Detection Mechanism:

- User states symptoms started 5 days before admission
- Medical records show emergency admission with acute onset
- AI interview follow-up questions reveal contradictions
- Sentiment analysis shows evasiveness when probed

System Response:

- Increase fraud risk score by 35 points
- Generate detailed timeline comparison report
- Escalate to senior adjuster for manual review
- Request additional medical documentation

6.3 Scenario 3: Provider Network Fraud Ring

Trigger: Multiple claims from same provider with similar patterns

Detection Mechanism:

- Graph database analysis identifies cluster of claims
- All claims submitted within 2-week window
- Unusually high claim amounts for similar diagnoses
- Provider has prior fraud flags in system
- AI detects similar phrasing across multiple claim interviews

System Response:

- Automatic hold on all related claims
- Generate network visualization for fraud unit

- Cross-reference with industry fraud database
- Initiate provider audit procedure

---

7. User Interface Specifications

7.1 Key Screens & Wireframes

Screen 1: Claim Entry Portal

```
╔═══════════════════════════════════════════════════════════╗
║ [Company Logo] Your Claim Portal ║
╠═══════════════════════════════════════════════════════════╣
║ ║
║ Welcome, [User Name] ║
║ Policy: ****5678 ║
║ ║
║ ┌─────────────────────────────────────────────┐ ║
║ │ Enter Policy Number │ ║
║ │ [_____] [Verify] │ ║
║ └─────────────────────────────────────────────┘ ║
║ ║
║ Progress: ●○○○○ ║
║ 1. Verify Policy 2. Upload 3. Interview ║
║ ║
╚═══════════════════════════════════════════════════════════╝
```

Screen 2: Document Upload Interface

```
╔═══════════════════════════════════════════════════════════╗
║ ← Back Upload Documents Help ║
╠═══════════════════════════════════════════════════════════╣
║ ║
║ Required Documents (3 of 5 uploaded) ║
║ ║
║ ✓ Hospital Bill [View] ║
║ ✓ Prescription [View] ║
║ ✓ Discharge Summary [View] ║
║ ⚠ Diagnostic Reports [Upload] ║
║ ○ Photo ID Proof [Upload] ║
║ ║
║ ┌─────────────────────────────────────────────┐ ║
║ │ Drag & Drop Files Here │ ║
║ │ or [Browse Files] │ ║
║ │ (PDF, JPG, PNG - Max 10MB each) │ ║
║ └─────────────────────────────────────────────┘ ║
║ ║
║ [Continue to Interview] → ║
╚═══════════════════════════════════════════════════════════╝
```

Screen 3: AI Conversational Interview

```
╔═══════════════════════════════════════════════════════════╗
║ ← Back Claim Interview (3 of 8 questions) ║
╠═══════════════════════════════════════════════════════════╣
║ ║
║  AI Assistant: ║
║ ┌─────────────────────────────────────────────┐ ║
║ │ I see you were hospitalized on │ ║
║ │ March 10. What symptoms led to │ ║
║ │ your admission? │ ║
║ └─────────────────────────────────────────────┘ ║
║ ║
║ Your Response: ║
║ ┌─────────────────────────────────────────────┐ ║
║ │ [Type your answer here...] │ ║
║ │ │ ║
║ │ │ ║
║ └─────────────────────────────────────────────┘ ║
║ ║
║ [ Speak] [Submit Answer] → ║
║ ║
║ Need help? [Chat with Agent] ║
╚═══════════════════════════════════════════════════════════╝
```

Screen 4: Admin Dashboard

```
╔═══════════════════════════════════════════════════════════════════════════╗
║ [Logo] Claims Dashboard [Search] [Profile] [Logout] ║
╠═══════════════════════════════════════════════════════════════════════════╣
║ ║
║ Claims Overview Today: Nov 21, 2025 ║
║ ┌──────────┬──────────┬──────────┬──────────┐ ║
║ │ Pending │ Review │ Approved │ Rejected │ ║
║ │ 247 │ 89 │ 156 │ 12 │ ║
║ └──────────┴──────────┴──────────┴──────────┘ ║
║ ║
║ High Priority Claims [Filter ▼] ║
║ ┌─────────────────────────────────────────────────────────────┐ ║
║ │ CLM-2025-4891 │ $18,500 │  High Risk │ [View] │ ║
║ │ CLM-2025-4889 │ $12,300 │  Review │ [View] │ ║
║ │ CLM-2025-4885 │ $9,800 │  High Risk │ [View] │ ║
║ └─────────────────────────────────────────────────────────────┘ ║
║ ║
║ Fraud Alerts (3 new) ║
║ • Duplicate document detected - CLM-2025-4891 ║
║ • Provider flagged - Dr. XYZ Clinic ║
║ • Timeline inconsistency - CLM-2025-4880 ║
║ ║
╚═══════════════════════════════════════════════════════════════════════════╝
```

7.2 Design System

- **Color Palette:**
  - Primary: #0066CC (trust blue)
  - Secondary: #28A745 (success green)
  - Alert: #DC3545 (warning red)
  - Neutral: #6C757D (gray)
- **Typography:**
  - Headings: Inter (sans-serif)
  - Body: System fonts for performance
  - Size: 16px base (accessible)
- **Components:** Consistent button styles, form inputs, cards, modals

---

8. Development Phases & Timeline

Phase 1: Foundation (Weeks 1-6)

Deliverables:

- Project setup (repos, CI/CD, environments)
- Database schema implementation
- Authentication system (JWT, OTP)
- Basic UI framework (Next.js + Tailwind)
- Policy validation API

Team: 2 backend, 2 frontend, 1 DevOps

Phase 2: Core Functionality (Weeks 7-14)

Deliverables:

- Document upload with S3 integration
- OCR integration (Azure Document Intelligence)
- Claim submission workflow
- Admin dashboard (basic view)
- Email/SMS notification system

Team: 3 backend, 3 frontend, 1 QA

Phase 3: AI Integration (Weeks 15-22)

Deliverables:

- Conversational AI interview module
- Fraud detection model (v1)
- AI response analysis
- Risk scoring algorithm
- Model monitoring dashboard

Team: 2 ML engineers, 2 backend, 1 data scientist

Phase 4: Testing & Compliance (Weeks 23-28)

Deliverables:

- HIPAA compliance audit
- Security penetration testing
- Load testing (10K concurrent users)
- Accessibility audit (WCAG 2.1 AA)
- UAT with pilot users (50 claims)

Team: 2 QA, 1 security engineer, 1 compliance officer

Phase 5: Launch & Optimization (Weeks 29-32)

Deliverables:

- Soft launch (limited user base)
- Production monitoring setup
- Bug fixes and optimizations
- User feedback integration
- Full production rollout

Team: Full team + support staff

---

9. Risk Assessment & Mitigation

9.1 Technical Risks

Risk	Probability	Impact	Mitigation Strategy
AI model inaccuracy	Medium	High	Ensemble models, human-in-loop for high-risk, continuous retraining
OCR extraction errors	Medium	Medium	Manual review fallback, confidence score thresholds, multi-vendor support
System downtime	Low	Critical	Multi-region deployment, auto-scaling, 24/7 monitoring
Data breach	Low	Critical	End-to-end encryption, regular audits, penetration testing, SOC 2 certification

9.2 Business Risks

Risk	Probability	Impact	Mitigation Strategy
User adoption resistance	Medium	High	Intuitive UX, onboarding tutorials, support team, gradual rollout
Regulatory non-compliance	Low	Critical	Legal review, compliance officer, regular audits, HIPAA training
False fraud accusations	Medium	High	Human review for all rejections, clear appeal process, explainable AI
High operational costs	Medium	Medium	Auto-scaling, serverless functions, cost monitoring, vendor negotiations

9.3 Ethical Considerations

- **Bias in AI Models:** Regular fairness audits to ensure no discrimination
- **Privacy:** Minimize data collection, clear consent forms, right to data deletion
- **Transparency:** Explain to users how AI is used in claim evaluation
- **Appeals Process:** Clear mechanism for disputing AI decisions

---

10. Success Criteria & KPIs

10.1 Launch Criteria (Go/No-Go Checklist)

- [ ] All critical functionality tested (>95% test coverage)
- [ ] HIPAA compliance certification obtained
- [ ] Security audit passed with no critical vulnerabilities
- [ ] Load testing confirms system handles 10K users
- [ ] Disaster recovery plan tested successfully
- [ ] Admin training completed
- [ ] Legal and privacy policies approved
- [ ] Customer support team trained

10.2 Post-Launch KPIs (Monthly Tracking)

Operational Metrics

- **Claim Volume:** Total claims submitted
- **Processing Time:** Average time from submission to decision
- **Auto-Approval Rate:** % of claims approved without human review
- **Fraud Detection Rate:** % of fraudulent claims caught
- **False Positive Rate:** % of legitimate claims flagged as fraud

Business Metrics

- **Cost per Claim:** Total operational cost / claims processed
- **Customer Satisfaction (CSAT):** Survey score (1-5 scale)
- **Net Promoter Score (NPS):** Likelihood to recommend
- **Claim Denial Rate:** % of claims rejected
- **Appeal Rate:** % of rejected claims appealed

Technical Metrics

- **System Uptime:** % availability
- **API Error Rate:** % of failed requests
- **Page Load Time:** 90th percentile response time
- **AI Model Accuracy:** Precision, recall, F1-score

10.3 Quarterly Review Goals

- **Q1:** Successfully process 1,000 claims with <5% error rate
- **Q2:** Reduce processing time to <48 hours for 80% of claims
- **Q3:** Achieve 85% fraud detection rate with <10% false positives
- **Q4:** Scale to 5,000 claims/month with maintained quality metrics

---

11. Budget & Resources

11.1 Technology Costs (Annual)

Category	Provider	Annual Cost (USD)
Cloud Infrastructure	AWS/Azure	$120,000
OCR Services	Azure Document Intelligence	$36,000
AI/ML APIs	OpenAI GPT-4	$60,000
Database	PostgreSQL RDS	$24,000
File Storage	S3 + CloudFront	$18,000
Monitoring & Logging	Datadog	$12,000
Security Tools	Penetration testing, WAF	$30,000
Total Technology		**$300,000**

11.2 Team Resources (6-month project)

Role	Count	Rate (USD/month)	Total Cost
Senior Backend Engineer	2	$12,000	$144,000
Senior Frontend Engineer	2	$11,000	$132,000
ML Engineer	2	$13,000	$156,000
DevOps Engineer	1	$11,000	$66,000
QA Engineer	1	$8,000	$48,000
Product Manager	1	$10,000	$60,000
UI/UX Designer	1	$9,000	$54,000
Compliance Officer	1	$10,000	$60,000
Total Team			**$720,000**

11.3 Total Project Budget

- **Development:** $720,000
- **Technology:** $150,000 (6 months)
- **Contingency (15%):** $130,500
- **Grand Total: $1,000,500**

11.4 ROI Projection (First Year)

- **Cost Savings:** $250,000 (reduced manual processing)
- **Fraud Prevention:** $180,000 (15% reduction in fraud payouts)
- **Total Benefit:** $430,000
- **Payback Period:** ~2.3 years

---

12. Appendices

Appendix A: Glossary

- **FNOL:** First Notice of Loss - initial claim report
- **OCR:** Optical Character Recognition - text extraction from images
- **PHI:** Protected Health Information - sensitive medical data
- **SLA:** Service Level Agreement - uptime/performance guarantees
- **WCAG:** Web Content Accessibility Guidelines

Appendix B: Regulatory References

- Health Insurance Portability and Accountability Act (HIPAA) - 45 CFR Parts 160, 162, and 164
- General Data Protection Regulation (GDPR) - for international users
- Payment Card Industry Data Security Standard (PCI DSS) - if processing payments

Appendix C: Research Citations

[1] Practolytics. (2025). "Best Practices for Insurance Verification 2025." https://practolytics.com/blog/best-practices-for-insurance-verification-2025/

[2] FlowForma. (2025). "Healthcare Claims Automation: Complete Guide 2025." https://www.flowforma.com/en-gb/blog/healthcare-claims-automation

[3] AutomationEdge. (2025). "Insurance Claim Fraud Detection Using Automation and AI." https://automationedge.com/blogs/insurance-claim-fraud-detection-using-ai-automation/

[4] Deloitte Insights. (2025). "Using AI to Fight Insurance Fraud." https://www.deloitte.com/us/en/insights/industry/financial-services

[5] CDC. (2024). "Health Insurance Portability and Accountability Act (HIPAA)." https://www.cdc.gov/phlp/php/resources/health-insurance-portability-and-accountability-act-of-1996-hipaa.html

[6] Microsoft Azure. (2024). "Document Intelligence Health Insurance Card Model." https://learn.microsoft.com/en-us/azure/ai-services/document-intelligence/prebuilt/health-insurance-card

[7] Veryfi. (2025). "Health Insurance Cards OCR API." https://www.veryfi.com/health-insurance-cards-ocr-api/

[8] Rasa. (2025). "Why Insurers Are Adopting Conversational AI." https://rasa.com/blog/conversational-ai-for-insurance

[9] Plivo. (2025). "How Insurance Chatbots Can Provide a Conversational Experience." https://www.plivo.com/blog/insurance-chatbots-conversational-experience/

Document Version History

Version	Date	Author	Changes
1.0	Nov 21, 2025	Product Team	Initial PRD creation

Approvals Required

- [ ] Product Manager
- [ ] Engineering Lead
- [ ] Compliance Officer
- [ ] Chief Information Security Officer (CISO)
- [ ] Chief Technology Officer (CTO)