International Journal of Core Engineering & Management
Volume-8, Issue-04, 2025 ISSN No: 2348-9510

SECURE CLOUD PLATFORMS WITH AI FOR AUTOMATED HEALTH INSURANCE CLAIM PROCESSING AND FRAUD DETECTION

Sai Nitesh Palamakula
Software Engineer
Microsoft Corporation
Charlotte, NC, USA
palamakulasainitesh@gmail.com

Abstract

The manual processing of health insurance claims is increasingly recognized as both slow and susceptible to fraud, burdening insurers with rising costs and customers with delayed reimbursements. To address these challenges, the convergence of secure cloud computing and agentic artificial intelligence (AI) systems has emerged as a transformative paradigm. This paper explores the design and implementation of secure, scalable cloud platforms leveraging AI for automated claim validation and robust fraud detection. Drawing on current research and industry deployments, it details architectural models employing microservices, real-time data ingestion, and explainable AI pipelines to enhance speed, accuracy, and resilience. Challenges surrounding integration with legacy systems, data privacy, regulatory compliance (particularly HIPAA), explainability, and ethical fairness are rigorously examined. The paper proposes a systematic evaluation strategy focusing on key performance indicators such as latency, detection accuracy, availability, and transparency. Case studies from cloud service providers, health payers, and AI vendors illustrate the operational value, while analysis of ongoing lawsuits and recent legal frameworks highlights the importance of transparency and patient-centered AI. The report concludes by pointing to future-proofed hybrid architectures, continuous learning models, and evolving benchmarks (such as HealthBench), establishing an actionable roadmap for secure, automated, and fair health insurance claim processing.

Index Terms – Secure Cloud, Health Insurance Claims, Agentic AI, Fraud Detection, Claims Automation, Data Encryption, HIPAA Compliance, Microservices, Predictive Analytics, Explainable AI, Real-Time Processing, Legacy System Integration, Evaluation Metric

I. INTRODUCTION

The health insurance industry has long been challenged by operational inefficiency and rampant fraud in claims processing. Historically, claim adjudication has entailed laborious manual checks, increasing the risk of errors, administrative delays, and financial leakage from undetected fraudulent patterns[1]. As claim volumes and complexities rise, and fraud strategies grow more sophisticated—including syndicate frauds, upcoding, duplicate billing, and identity manipulation—the inadequacies of manual and static rule-based systems become acute[2].

Recent advances in cloud computing and artificial intelligence—particularly agentic AI capable of context-aware, autonomous, and adaptive decision-making—present a unique opportunity for insurers to streamline claim processes, enhance customer experience, and sharply curtail fraudrelated losses. Cloud platforms provide the scalability, security, and interoperability necessary for ingesting vast, heterogeneous medical and claims data, while AI automates validation and fraud detection, offering real-time triage and explainable flagging [3][4].

However, these advances come with technical and socio-ethical considerations. Large-scale, automated handling of sensitive personal health information (PHI) introduces new vectors for data breach and requires strict adherence to healthcare privacy regulations such as HIPAA[5][6]. Furthermore, AI models—if inadequately governed—may encode bias, lack explainability, or amplify systemic inequities in claim adjudication and fraud detection.

This paper delves into the technological, operational, and regulatory facets of building secure, AI-powered cloud platforms for automated health insurance claim processing and fraud detection. We outline state-of-the-art architectures, implementation practices, evaluation methodologies, and address the major challenges and limitations. Recent industry cases, benchmarks, and legal disputes are critically examined to chart a comprehensive path towards trustworthy and scalable solutions in this dynamic field.

II. PURPOSE AND SCOPE

A. Purpose

The purpose of this paper is to provide a rigorous, technical analysis of secure cloud platforms augmented with agentic AI for automating health insurance claim validation and fraud detection. It aims to:

- Illustrate the architectural patterns and technical choices for building such platforms.
- Survey the AI algorithms used for fraud detection and automated claim adjudication.
- Assess cloud security frameworks and key management practices relevant to healthcare data.
- Examine regulatory and compliance obligations-specifically HIPAA-for cloud-based health systems.
- Propose comprehensive implementation and evaluation strategies.
- Analyze challenges, ethical considerations, and limitations in operationalizing these solutions.
- Offer guidance for integrating (and migrating) legacy claim systems into modern AI-driven cloud platforms.

B. Scope

The scope of this study includes:

- Health insurance domains (claims management and fraud detection) as opposed to broader general insurance.
- Solutions employing secure public, private, or hybrid cloud architectures with robust encryption, monitoring, and compliance frameworks.
- Agentic and explainable AI systems (including supervised learning, anomaly detection, graph analytics, and advanced language models) as core automation enablers.
- Pipelines enabling real-time or near real-time claims scoring and fraud detection.
- Integration and interoperability with legacy systems using standard APIs, RPA, or orchestration layers.

III. RELATED WORK

The intersection of cloud computing, AI, and health insurance claim processing has been an active research area over the past decade, marked by increasing sophistication in both fraud schemes and counter measures.

A. AI Fraud Detection and Automated Claims

Research has shown that AI-driven predictive analytics and real-time models can boost claims fraud detection accuracy by up to 30% over static rule systems, with notable cost reduction and improved operational efficiency[7][8]. Pioneering companies such as SAS, H2O.ai, and LexisNexis have deployed machine learning solutions that leverage structured and unstructured data to detect new fraud modalities and enable straight-through processing. These systems use techniques ranging from traditional supervised learning (e.g., logistic regression, random forests) to advanced anomaly detection, deep networks, and graph-based methods for identifying provider collusion and networked fraud.

Recent literature highlights the rise of "agentic" AI—intelligent agents capable of continuous, adaptive monitoring and decision support—marking a departure from periodic batch analysis towards real-time, context-aware fraud prevention. These systems autonomously validate claims against both policy rules and historical patterns, escalate suspicious events, and enable efficient triage for human review [9][10].

B. Cloud-Native Security and Regulatory Compliance

Parallel to AI advances, the migration from on-premise to cloud-native infrastructures has underpinned new levels of scalability, agility, and cost efficiency in healthcare IT[11][1]. Cloud adoption has been associated with improved uptime, disaster recovery, and the ability to meet surge demand, especially during health crises (e.g., COVID-19).

Security and compliance are central concerns for healthcare deployments. Best practices and frameworks for HIPAA compliance in cloud environments involve robust encryption, access controls, multi-factor authentication, audit logging, and incident response planning[12][5][13][14]. Issues specific to multi-cloud involve data fragmentation, inconsistent controls, and vendor risk management, with emerging solutions in centralized monitoring, DLP, and federated key management [14][15][13].

C. Legal, Ethical, and Socio-Technical Challenges

The legal landscape is rapidly evolving. Class-action lawsuits filed against major insurers have catalysed scrutiny of algorithmic opacity, bias, and wrongful denials, highlighting the need for explainable, patient-cantered AI and regulatory oversight[21][22][23]. Ethical frameworks now underscore the need for robust model transparency, bias mitigation, patient autonomy, and human oversight in automated claim decisions.

IV. SYSTEM ARCHITECTURE

The reference architecture for secure, cloud-based, AI-driven health insurance claim processing must balance four key requirements: efficiency, scalability, security, and compliance. Modern solutions converge on the following layered model, shown in the Fig. 1. This layered, modular architecture supports scalability, resilience, and transparency. Microservices, API orchestration, and feature stores enable flexible deployment and integration across both cloud-native and on-premise (legacy) systems. Embedding explainability and compliance into the workflow ensures regulatory adherence and fosters stakeholder trust. Integration with robust cloud security stacks (such as AWS HealthLake, Azure Health Data Services, Google Vertex AI) allows for rapid scaling, disaster recovery, and continuous deployment without sacrificing data integrity or privacy [24][25].

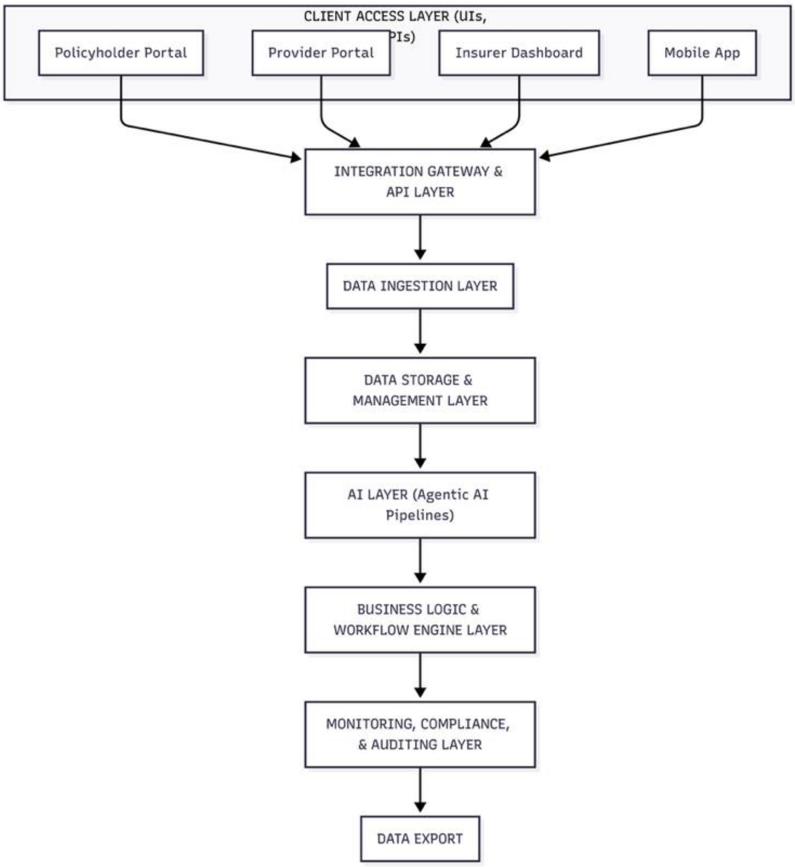
CLIENT ACCESS LAYER (UIs,
PIs)
Policyholder Portal
Provider Portal
Insurer Dashboard
Mobile App
INTEGRATION GATEWAY & API LAYER
DATA INGESTION LAYER
DATA STORAGE & MANAGEMENT LAYER
AI LAYER (Agentic AI Pipelines)
BUSINESS LOGIC & WORKFLOW ENGINE LAYER
MONITORING, COMPLIANCE, & AUDITING LAYER
DATA EXPORT

Fig. 1.High Level Architecture for Secure, Agentic AI-Driven Claim Processing Platform

A. Fraud Detection Subsystem

The Fraud Detection Subsystem analyzes claims using ensemble ML models, anomaly detection, and graph-based provider–patient networks. It outputs a fraud risk score, alerts, and explanations to flag suspicious claims for review. It is visualized in Fig. 2.

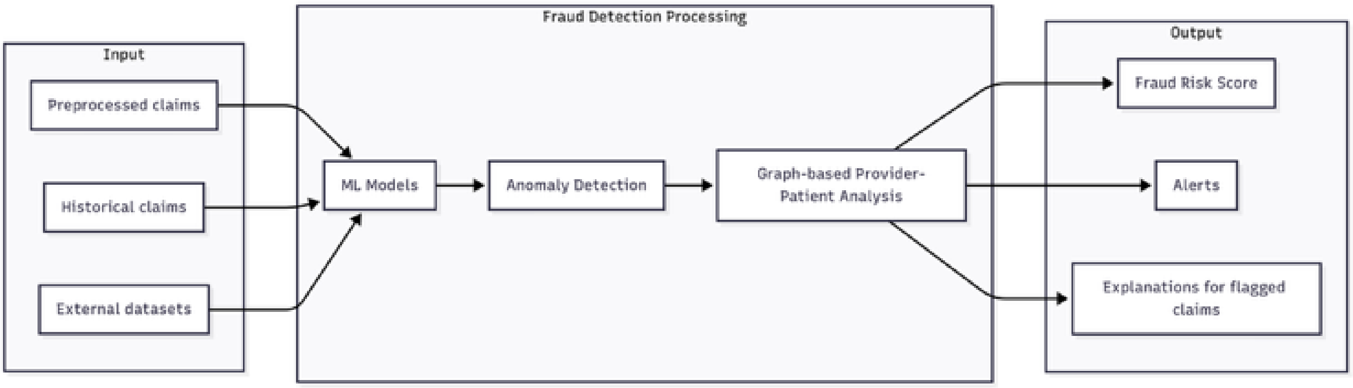

Fig. 2. Fraud Detection Subsystem

B. Claim Validation Subsystem

The Claim Validation Subsystem uses NLP and rule-based checks to validate new claims against policy and provider data, ensuring eligibility and detecting duplicates. It delivers a fast adjudication outcome, automatically routing claims for payment or escalation. It is visualized in Fig. 3.

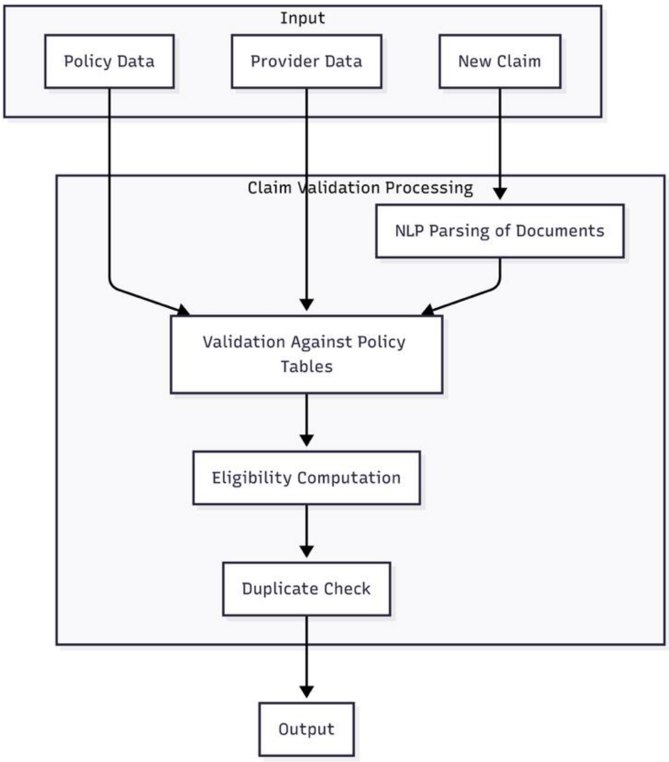

Fig. 3. Claim Validation Subsystem

C. Security and Compliance Subsystem

The Security and Compliance Subsystem safeguards data in motion and at rest through encryption, access logging, and periodic audits. It generates audit logs and incident reports to support monitoring and regulatory compliance. It is visualized in Fig. 4.

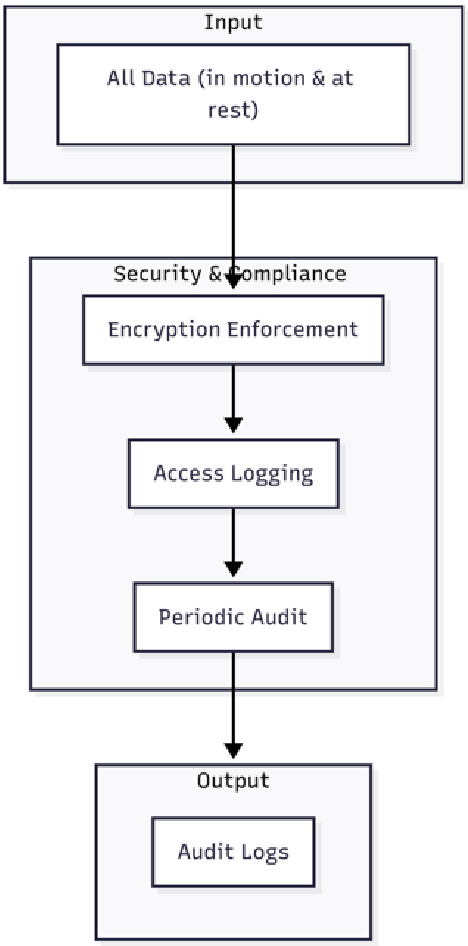

Fig. 4. Security and Compliance Subsystem

V. IMPLEMENTATION

A. AI Pipelines for Claims Processing

Automated claims processing leverages AI pipelines that blend supervised, unsupervised, and deep learning models trained on historical claims data. These pipelines process the claim lifecycle through several automated stages:

- **Ingestion and Preprocessing**: AI engines use OCR, NLP, and entity extraction to parse claims documents, medical bills, and attached evidence (images, PDFs, etc.). Models correct inconsistencies and validate schema compliance.
- **Claim Validation**: Contextual logic and policy tables are applied using ontology-based algorithms, flagging out-of-policy or incomplete claims for further review [26].
- **Fraud Risk Scoring**: Multiple algorithms run in ensemble:
    - Random Forest, XGBoost, and DNNs for behavior pattern and anomaly detection.
    - Graph neural networks and community detection for collusive fraud, using

provider patient relationship graphs[27][28].
  - Clustering (e.g., DBSCAN, k-means) and One-Class SVM for unsupervised outlier detection.

- **Explainability and Human-in-the-Loop**: Flagged claims are passed with explainable outputs (e.g., SHAP, LIME) for human supervisor review and intervention [8].
- **Adaptive Learning**: Models integrate feedback from investigators and claim payout decisions. Versioning and A/B testing are routinely applied to avoid concept drift.

B. Cloud Security and Data Protection

Cloud infrastructures are configured via best practice security frameworks, including:

- Encryption
- Access Control
- Audit Logging and Monitoring
- Data Governance

C. Legacy System Integration

Integration frameworks utilize robotic process automation (RPA), middleware API gateways, and orchestration layers (as documented by Acceltree and Sprout.ai) to bridge monolithic, batch-oriented legacy claim systems with real-time cloud architecture, enabling non-invasive modernization [29][30]

VI. EVALUATION STRATEGY

A robust evaluation framework for AI-driven, cloud-based health claims processing must encompass the following metrics. Table I provides an overview of the key evaluation metrics

TABLE I. EVALUATION METRICS

Metric	Description
Completion Average claim cycle time	Time from claim submission to payout/denial
Throughput (claims/hr)	Claims processed per unit time under peak demand
Accuracy, Recall, AUC	Ability to correctly flag fraudulent claims and minimize false positives/negatives
Explainability rate	Percentage of work items completed without need for rework/re-submission
Uptime/Resilience	% time system is fully operational; mean time to recovery (MTTR)
Breach rate, audit pass	Incidents of unauthorized access; audit compliance
Regulatory alignment	Conformance to HIPAA, GDPR, SOC-2, etc.

Each metric is continuously monitored using cloud-native observability dashboards (e.g., Azure Monitor, Amazon CloudWatch, Grafana, Prometheus), ensuring performance tracking and real-time system reporting.

VII. TECHNICAL CONSIDERATIONS

A. Cloud Security and HIPAA Compliance

Among the most critical considerations in healthcare AI are data security and regulatory compliance. HIPAA (US) and GDPR (EU) set strict technical safeguards, including:

- **Encryption:** All PHI must be encrypted both in transit (TLS 1.2 or higher) and at rest, with centralized key management and strong key rotation policies [12][15].
- **Access Control**: Role-based and least-privilege access, enforced multi-factor authentication, and segregation of duties for administrators and data scientists; identity and access management (IAM) is audited for every access event.
- **Audit Trails**: Immutable logging of all policy, data, and model access is a must, with logs retained per regulatory timelines and available for incident investigation.
- **Data Localization**: Some cloud providers offer regional storage guarantees for sensitive data, adhering to 'data residency' requirements of HIPAA and local laws.

B. Data Management and Pipeline Architecture

- **Data Integration**: Claims, EHR, policy, provider, and external (e.g., social media for fraud signals) data require real-time ETL or change data capture (CDC) connectors. Feature stores (for AI models) manage pipeline feature stability and retraining workflows.
- **Serverless and Containerization**: Utilizing platforms such as AWS Lambda, Azure Functions, or Kubernetes microservices supports efficient scaling, rapid deployment, and isolation of workloads.
- **Performance Optimization**: Techniques such as model quantization, in-memory caching, and efficient batch/streaming pipelines are used to minimize latency and optimize resource utilization [3].

VIII. CHALLENGES AND LIMITATIONS

Despite significant advances, there remain substantial challenges to adoption and operationalization:

A. Technical

- **Legacy Systems**: Overcoming technical debt and data silos in legacy claim platforms can impede integration; API gateways, middleware, and RPA are workarounds but add complexity[29][30].
- **Data Quality**: Claims and medical data are prone to errors, missingness, and non-standard coding across providers. Pipelines must regularly validate, impute, and reconcile source data.
- **Model Performance and Drift**: Imbalanced datasets (fraud is rare), evolving fraud tactics, and adversarial attacks can undermine AI detection reliability. Real-time retraining and robust validation pipelines are essential[31][28].

B. Security and Compliance

- **Multi-Cloud Complexity**: Enforcing uniform security, encryption, and audit across multiple cloud vendors introduces risk; compliance stacks must be harmonized and centralized across all environments[14][13].
- **Auditability and Explainability**: Regulatory and legal scrutiny of claim denials demands that payers can provide understandable, traceable AI-driven decisions.

C. Legal and Ethical

- **Transparency:** Recent lawsuits and regulatory scrutiny underscore the need to avoid 'black box' AI claim denials[21][23]. Both providers and claimants expect human-understandable justifications.
- **Bias and Fairness:** AI models may inadvertently propagate or amplify pre-existing disparities if not carefully balanced and audited [6].

IX. CONCLUSION

Secure cloud platforms enhanced with agentic AI represent a paradigm shift for health insurance claim processing and fraud detection. By automating claims adjudication, delivering real-time fraud risk scoring, and guaranteeing transparent, explainable, and compliant workflows, these architectures offer a path to faster, more accurate, and fairer claim settlements.

The technical foundation demands robust, modular cloud architectures, strong security frameworks enforcing HIPAA and regional compliance, and advanced AI pipelines blending prediction, detection, and explainability. Integration with legacy systems, continuous security management, and effective human-AI collaboration are vital for real-world success. Operational metrics must balance throughput, detection accuracy, system resilience, and user trust.

While challenges in data quality, integration, security, and bias remain, the demonstrable benefits—reduced fraud, lower total cycle time, improved customer satisfaction, and enhanced regulatory oversight—affirm the value proposition. As regulatory, legal, and ethical landscapes evolve, continuous improvement in explainability, fairness, and hybrid human oversight will determine long-term acceptance and value.

Widespread adoption will hinge on continued partnership between healthcare payers, IT and cloud vendors, AI providers, and regulators to ensure these systems remain secure, trustworthy, and centered on the needs of both patients and insurers. The foundation is set for a future of health insurance where claims are processed swiftly, accurately, and justly—guided by secure, intelligent systems designed for resilience, fairness, and transparency.

REFERENCES

1. Oracle, “Oracle unveils cloud-based solution to transform healthcare claims,” Cloud Curated, Oct. 2024. [Online]. Available: https://cloudcurated.com/oracle-healthcare-claims
2. Neutrinos, “AI agents in insurance fraud prevention,” Neutrinos Resource Hub, Aug. 2025. [Online]. Available: https://resources.neutrinos.co/insurance-fraud-ai

3. Inaza, AI and Predictive Analytics in Claims Automation Explained, Feb 2025. [Online]. Available: https://inaza.ai/blog/claims-automation-ai
4. Amazon Web Services, "Modernizing healthcare data platforms for generative AI," Aug. 2025. [Online]. Available: https://aws.amazon.com/blogs/healthcare/modernizing-healthcare-data-platforms
5. Insurance Glossary, "Insurance fraud detection AI: Modern approaches, risks, and industry impact," Jul. 2025. [Online]. Available: https://insuranceglossary.org/fraud-detection-ai
6. DICEUS, "AI in health insurance: Use cases and key challenges," Sep. 2024. [Online]. Available: https://diceus.com/blog/ai-health-insurance
7. R. Goyal, "Combatting fraud in insurance claims using advanced analytics," IJMRGE, Sept. 2024.
8. Amazon Web Services, "Modernizing healthcare data platforms for generative AI," Aug. 2025. [Online]. Available: https://aws.amazon.com/blogs/healthcare/modernizing-healthcare-data-platforms
9. Kellton, "Agentic AI insurance claims processing and management: The benefits and use cases," Aug. 2025. [Online]. Available: https://www.kellton.com/blogs/agentic-ai-insurance-claims
10. HIPAA Vault, "Top 10 security best practices for HIPAA-compliant cloud hosting," Mar. 2025. [Online]. Available: https://www.hipaavault.com/blog/hipaa-cloud-security-best-practices
11. Orca Security, "HIPAA compliance guide: Cloud security & healthcare data protection," 2025. [Online]. Available: https://orca.security/resources/hipaa-cloud-compliance-guide
12. TrustCloud, "HIPAA compliance in multi-cloud environments: Challenges and solutions," Jun. 2025. [Online]. Available: https://trustcloud.ai/blog/hipaa-multicloud-compliance
13. Kellton, "Agentic AI insurance claims processing and management (Extracted)," Aug. 2025. [Online]. Available: https://www.kellton.com/blogs/agentic-ai-insurance-claims
14. ML Journey, "Agentic AI use cases in insurance: Transforming claims, risk, and customer experience," Jun. 2025. [Online]. Available: https://mljourney.ai/agentic-ai-insurance-use-cases
15. Xenonstack, "Agentic AI insurance claims (Extracted)," Apr. 2025. [Online]. Available: https://www.xenonstack.com/blog/agentic-ai-insurance-claims
16. MDPI, "Health insurance fraud detection using machine and deep learning analytics," 2025. [Online]. Available: https://www.mdpi.com/healthcare-fraud-detection-ml
17. IJFMR, "Healthcare fraud detection using ML and AI," May. 2024. [Online]. Available: https://www.ijfmr.com/papers/healthcare-fraud-detection-ml-ai
18. Langate, "Insurance fraud detection using machine learning," Feb. 2025. [Online]. Available: https://www.langate.com/blog/ml-insurance-fraud-detection
19. Onlinescientificresearch, "Scalable cloud architectures for deploying AI applications," 2025. [Online]. Available: https://onlinescientificresearch.com/cloud-ai-architecture
20. Datwave, "Cloud AI architecture: Scalable AI and HPC solutions," 2024–2025. [Online]. Available: https://datwave.ai/resources/cloud-ai-architecture
21. YASH Technologies, "Building scalable AI solutions with cloud infrastructure: Best practices," Dec. 2024. [Online]. Available: https://www.yash.com/blogs/scalable-ai-cloud
22. Unicloud, "How to secure healthcare data on cloud: A technical guide," Oct. 2023. [Online]. Available: https://www.unicloud.io/blog/secure-healthcare-data-cloud

23. DuoKey, "Healthcare data protection – Cloud encryption & key management," 2025. [Online]. Available: https://duokey.com/blog/healthcare-data-encryption
24. Randtronics, "Protecting patient records with healthcare data encryption solutions," Jun. 2025. [Online]. Available: https://www.randtronics.com/blog/patient-records-encryption
25. Simbo.ai, "Utilizing Azure AI services for HIPAA-compliant healthcare solutions: Best practices and recommendations," 2025. [Online]. Available: https://simbo.ai/blog/azure-ai-hipaa-healthcare
26. Dymin Systems, "AI and HIPAA: Risks and how to stay compliant," May. 2025. [Online]. Available: https://www.dyminsystems.com/blog/ai-hipaa-compliance
27. Foley, "HIPAA compliance for AI in digital health: What privacy officers need to know," May. 2025. [Online]. Available: https://www.foley.com/en/insights/publications/2025/05/hipaa-compliance-ai-digital-health
28. EA Journals, "Real-time AI for financial claims processing: Architecture and implementation," Jun. 2025. [Online]. Available: https://eajournals.org/real-time-ai-claims-processing
29. Google Cloud, "Insurance claim processing reference architecture," Jan. 2023. [Online]. Available: https://cloud.google.com/architecture/insurance-claims-processing
30. EA Journals, "Real-time AI for financial claims processing: Architecture and implementation," Jun. 2025. [Online]. Available: https://eajournals.org/real-time-ai-claims-processing
31. Markovate, "AI in claims processing: Boosting efficiency and accuracy," May. 2025. [Online]. Available: https://www.markovate.com/blog/ai-in-claims-processing
32. Confluent, "Insurance claims stream processing," Sept. 2024. [Online]. Available: https://www.confluent.io/blog/insurance-claims-stream-processing
33. EA Journals, "Real-time AI for financial claims processing: Architecture and implementation," Jun. 2025. [Online]. Available: https://eajournals.org/real-time-ai-claims-processing
34. Ultralytics, "Accuracy vs. precision vs. recall in machine learning," Aug. 2025. [Online]. Available: https://docs.ultralytics.com/guides/accuracy-vs-precision-vs-recall
35. N. Prova, "Healthcare fraud detection using ML and AI," Pace University, 2024. [Online]. Available: https://digitalcommons.pace.edu/student_projects/healthcare-fraud-ml
36. Number Analytics, "Applications and challenges of precision-recall curves explained," Mar. 2025. [Online]. Available: https://numberanalytics.com/blog/precision-recall-curves
37. MITRIX, "AI and healthcare: LLMs, HealthBench, and what the future holds," May. 2025. [Online]. Available: https://mitrix.ai/blog/ai-healthcare-healthbench
38. OpenTools.ai, "OpenAI's HealthBench: Revolutionizing healthcare AI benchmarking," May. 2025. [Online]. Available: https://opentools.ai/blog/openai-healthbench
39. OpenAI, "HealthBench overview: AI evaluation for human health," May. 2025. [Online]. Available: https://openai.com/research/healthbench-overview
40. Sutherland, "Revolutionizing claims with AI: From legacy systems to automation," Mar. 2025. [Online]. Available: https://www.sutherlandglobal.com/insights/ai-claims-automation
41. Sprout.ai, "Just how difficult is it to integrate AI with legacy insurance systems?," Nov. 2024. [Online]. Available: https://sprout.ai/blog/integrating-ai-legacy-systems

42. Acceltree, "Claims orchestration layer for legacy systems," 2023–2025. [Online]. Available: https://acceltree.com/solutions/claims-orchestration-layer
43. OpenTools.ai, "AI algorithms in healthcare: Are insurers overstepping bounds," 2025. [Online]. Available: https://opentools.ai/blog/ai-healthcare-insurers-boundaries
44. Gianelli & Morris, "How AI is failing insureds: The dark side of automation in health insurance," Jan. 2025. [Online]. Available: https://gianellimorris.com/blog/ai-health-insurance-failures
45. Bloomberg Law, "AI, algorithm-based health insurer denials pose new legal threat," Apr. 2025. [Online]. Available: https://news.bloomberglaw.com/health-law-and-business/ai-health-insurer-denials-legal-threat
46. Confluent, "Insurance claims stream processing," Sept. 2024. [Online]. Available: https://www.confluent.io/blog/insurance-claims-stream-processing
47. Microsoft, "Transform insurance industry workflows using generative AI models and Azure services," Dec. 2024. [Online]. Available: https://learn.microsoft.com/en-us/industry/insurance/generative-ai-workflows
48. EA Journals, "Real-time AI for financial claims processing: Architecture and implementation," Jun. 2025. [Online]. Available: https://eajournals.org/real-time-ai-claims-processing
49. Devdiscourse, "AI-powered fraud detection system targets high-risk medical insurance abuse," Aug. 2025. [Online]. Available: https://www.devdiscourse.com/article/technology/ai-fraud-detection-healthcare
50. IJRIT, "Artificial intelligence in health insurance claims processing and fraud detection," Apr. 2025. [Online]. Available: https://www.ijrit.com/ai-health-insurance-claims-processing
51. Deloitte, "Using AI to fight insurance fraud," Apr. 2025. [Online]. Available: https://www2.deloitte.com/insights/ai-insurance-fraud
52. IBM, "Cloud-based insurance claim," 2021. [Online]. Available: https://www.ibm.com/cloud/insurance-claims
53. Virtusa, "Transform insurance claims processing with AI and automation," 2025. [Online]. Available: https://www.virtusa.com/insights/ai-insurance-claims
54. SparkNav, "How to use AI for claims processing in insurance," Sept. 2024. [Online]. Available: https://www.sparknav.com/blog/ai-claims-processing