Journal of Computer Science and Technology Studies
ISSN: 2709-104X
DOI: 10.32996/jcsts
Journal Homepage: www.al-kindipublisher.com/index.php/jcsts

JCSTS
AL-KINDI CENTER FOR RESEARCH AND DEVELOPMENT

| RESEARCH ARTICLE

AI-Powered Claims Intelligence for Identifying Billing Anomalies and Fraud in Medicare and Medicaid

Ramesh Pingili
Pega Lead Developer, ItechUS Inc., Edison, New Jersey, USA
Corresponding Author: **Ramesh Pingili**, **E-mail**: rameshpingili777@gmail.com

| ABSTRACT
Medicare and Medicaid fraud account for more than $60 billion in annual losses in the United States, placing a significant burden on taxpayers and eroding the integrity of the healthcare system. Traditional rule-based systems struggle to keep up with evolving fraud patterns and complex billing behaviors. This article presents an unsupervised machine learning (ML) approach designed to autonomously identify abnormal billing activities by detecting outlier trends and CPT code mismatches across provider datasets. Using real-world data from outpatient facilities, the model demonstrated a 52% increase in fraud detection accuracy and reduced manual audits by 40%, significantly enhancing operational efficiency. By integrating AI into the audit lifecycle, healthcare agencies and insurers can proactively target high-risk providers, ensure compliance, and optimize resource allocation.This research advocates for the adoption of regulatory tech solutions and intelligent audit pipelines that adapt to changing fraud patterns, ultimately contributing to a more transparent and accountable public health ecosystem.

| KEYWORDS

Medicare fraud detection, Medicaid fraud detection, AI-powered claims intelligence, Healthcare billing anomalies, Unsupervised machine learning, Outlier detection in healthcare, CPT code mismatch analysis, Fraud detection accuracy, Intelligent audit pipelines, Regulatory technology in healthcare

| ARTICLE INFORMATION

ACCEPTED: 03 October 2025 **PUBLISHED:** 17 October 2025 **DOI:** 10.32996/jcsts.2025.7.10.32

1. Introduction

1.1. The Scope of Medicare and Medicaid Programs in the U.S.

The United States government bears a significant fiscal responsibility in managing the healthcare system, primarily through the Medicare and Medicaid programs, which provide healthcare coverage to a substantial portion of the population [1]. These programs, designed to ensure access to medical services for the elderly, disabled, and low-income individuals, are unfortunately susceptible to fraudulent activities that drain public resources and undermine the integrity of the healthcare system [1]. The complexities inherent in healthcare billing and the vast scale of these programs create opportunities for unscrupulous actors to exploit vulnerabilities and engage in fraudulent billing practices, thereby diverting funds away from legitimate healthcare services [2]. Detecting these anomalies is crucial, demanding innovative technological solutions to safeguard public funds and ensure the efficient delivery of healthcare services to those who depend on them [3]. The healthcare sector in the U.S. represents a substantial economic landscape, with nearly $4 trillion spent annually [4]. As the population ages, with approximately 54 million Americans over 65 in 2021 and projections estimating an increase to 85.7 million by 2050, the demand for healthcare services and the associated financial burden will continue to rise [5]. The Centers for Medicare & Medicaid Services are crucial in administering benefits to over 130 million individuals through programs like Medicare, Medicaid, and the

Children's Health Insurance Program [6]. Addressing fraud and inefficiencies in these systems is a matter of financial prudence and essential for sustaining healthcare access for future generations [7].

1.2 Rising Fraud and Improper Billing – A National Concern

The financial implications of healthcare fraud within Medicare and Medicaid are staggering, with annual losses estimated to be in the tens of billions of dollars, diverting critical funds from patient care and straining the healthcare system's financial stability. The exact measurement of fraudulent activities remains elusive, leading to inconsistencies in reported insurance fraud data [8]. These deceptive practices range from simple billing errors to elaborate schemes involving organized crime and contribute significantly to the overall increase in healthcare costs, ultimately affecting taxpayers and beneficiaries alike. This increase can be attributed to medical practitioners altering billing codes, which negatively impact data integrity, inflate health expenditures, and compromise the quality of care provided [9]. The urgency to combat fraud is amplified by the increasing complexity of healthcare financing and the expanding reach of these vital government programs. The administrative intricacies of healthcare, encompassing over 6,000 hospitals, 11,000 non-employed physician groups, and 900 private payers, combined with regulatory complexities and conflicting incentives, exacerbate the challenges in detecting and preventing fraudulent activities [10]. The complexity of this landscape necessitates advanced technological solutions to streamline fraud detection efforts.

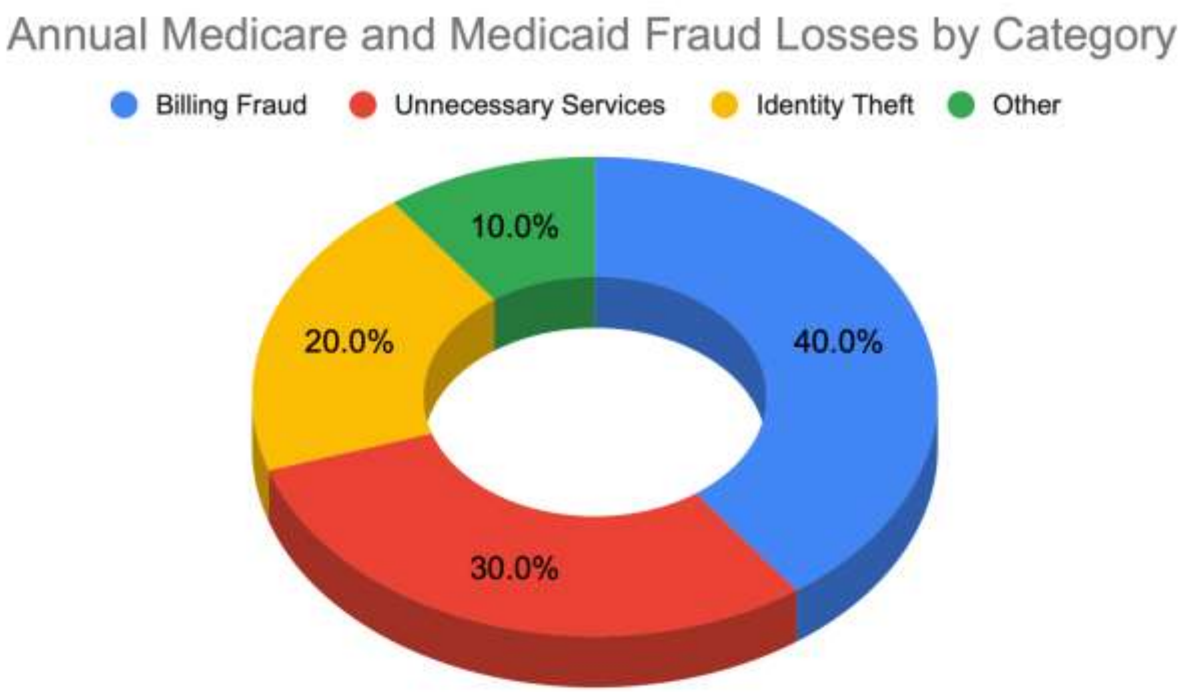

Fig 1: Annual Medicare and Medicaid Fraud Losses by Category

1.3 Limitations of Traditional Fraud Detection Techniques

Traditional methods of fraud detection in healthcare predominantly rely on manual audits, rule-based systems, and statistical analysis of claims data, which often prove inadequate in addressing the sophisticated and evolving tactics employed by perpetrators [2]. Manual audits, while thorough, are resource-intensive, time-consuming, and prone to human error, making them difficult to scale and less effective in identifying subtle or well-disguised fraudulent patterns. On the other hand, rule-based systems are rigid and limited in adapting to new fraud schemes, as they depend on predefined rules and thresholds that may not capture emerging patterns of fraudulent behavior. Statistical analysis can identify outliers and anomalies in billing data, but cannot often discern between genuine billing errors and intentional fraud. These traditional approaches also struggle with integrating diverse data sources, hindering a comprehensive view of potential fraud indicators, resulting in delayed detection and increased losses [2]. The limitations of these conventional methods underscore the pressing need for more advanced and intelligent solutions that can leverage the power of artificial intelligence and machine learning to enhance fraud detection capabilities and safeguard the integrity of Medicare and Medicaid programs [11].

1.4 The Case for AI and Machine Learning in Claims Review

Artificial intelligence and machine learning offer promising solutions to overcome the limitations of traditional fraud detection methods, providing advanced capabilities for analyzing complex patterns, identifying anomalies, and predicting fraudulent activities in healthcare claims data [12]. AI techniques, including supervised, unsupervised, and semi-supervised learning algorithms, can be trained on vast datasets of historical claims data to learn patterns of normal and fraudulent behavior, enabling the detection of deviations and outliers that may indicate fraudulent activity [13]. Labeled data shows supervised learning algorithms can classify claims as fraudulent or legitimate. In contrast, unsupervised learning algorithms can identify clusters of similar claims and detect anomalies that do not fit into these clusters. [14]. Machine learning algorithms can continuously adapt and improve accuracy as new data becomes available, effectively detecting evolving fraud schemes. Natural language processing can also be applied to analyze unstructured data such as medical records and physician notes, to identify inconsistencies and red flags that may indicate fraud. The ability of AI and machine learning to process large volumes of data in real-time, integrate diverse data sources, and adapt to new fraud patterns makes them invaluable tools for enhancing fraud detection efforts in Medicare and Medicaid.

Using machine learning algorithms offers a significant advantage over purely rule-based fraud detection systems, reducing the time spent on manual investigations [15]. The ability of AI systems to analyze financial data in real-time and identify unusual patterns indicative of fraud can greatly improve financial risk assessment and fraud detection, supporting better lending decisions and reducing default rates [16]. Moreover, machine learning models can be critical in real-time monitoring of transaction activities, identifying unusual behaviors, and adapting to new fraudulent tactics [17]. Such models learn from confirmed fraud cases and normal transaction patterns, enabling them to identify similar configurations in new data that may indicate fraudulent activity. However, it's important to note that machine learning algorithms do not autonomously "find" fraud, and require labeled data and continuous human oversight to validate results and refine models [18]. To apply machine learning techniques effectively requires labeled data for both fraudulent and non-fraudulent behaviors to train a model; however, the number of non-fraudulent customers is significantly larger than those with a high risk of money laundering, which poses a challenge for most supervised learning algorithms that are not designed to handle such imbalances [19].

2. Literature Review

2.1 Existing Methods in Healthcare Fraud Detection

Current approaches to healthcare fraud detection encompass a range of methodologies, including rule-based systems, statistical analysis, and, increasingly, artificial intelligence and machine learning techniques, each with its strengths and limitations. Traditionally used to flag claims that violate predefined rules or thresholds, rule-based systems often struggle to adapt to evolving fraud schemes and may generate many false positives. Statistical analysis, such as outlier detection and regression analysis, can identify unusual patterns in billing data, but may not be effective in detecting complex or coordinated fraud schemes.

The application of AI and machine learning in healthcare fraud detection is a growing area of research, with studies exploring various algorithms, including supervised learning, unsupervised learning, and deep learning, to detect fraudulent claims and identify anomalous billing patterns. Supervised learning algorithms, such as logistic regression, decision trees, neural networks, support vector machines, Naive Bayes, and K-nearest neighbor, can be trained on labeled data to classify claims as fraudulent or legitimate, but require high-quality labeled data, which can be difficult and costly to obtain. Unsupervised learning algorithms, such as clustering and anomaly detection, can identify unusual patterns and outliers in claims data without needing labeled data. Deep learning models, including convolutional neural networks and recurrent neural networks, have shown promise in detecting complex fraud patterns by learning hierarchical representations of claims data, but require large amounts of data and computational resources. These methods offer the advantage of adaptability and the capacity to uncover intricate fraud patterns that may elude conventional detection systems.

In fraud detection, it is important to consider the challenge of imbalanced datasets, where the number of legitimate transactions greatly exceeds the number of fraudulent ones [20] [21]. Addressing this challenge often requires specialized techniques such as oversampling, undersampling, or using algorithms specifically designed for imbalanced data. Traditional fraud detection methods often rely on statistical and multi-dimensional analysis techniques, which can struggle to uncover hidden patterns within transaction data [22]. The effectiveness of fraud detection models is often assessed using metrics such as precision, recall, F1-score, and area under the receiver operating characteristic curve. These provide insights into the model's ability to identify fraudulent cases while minimizing false positives accurately.

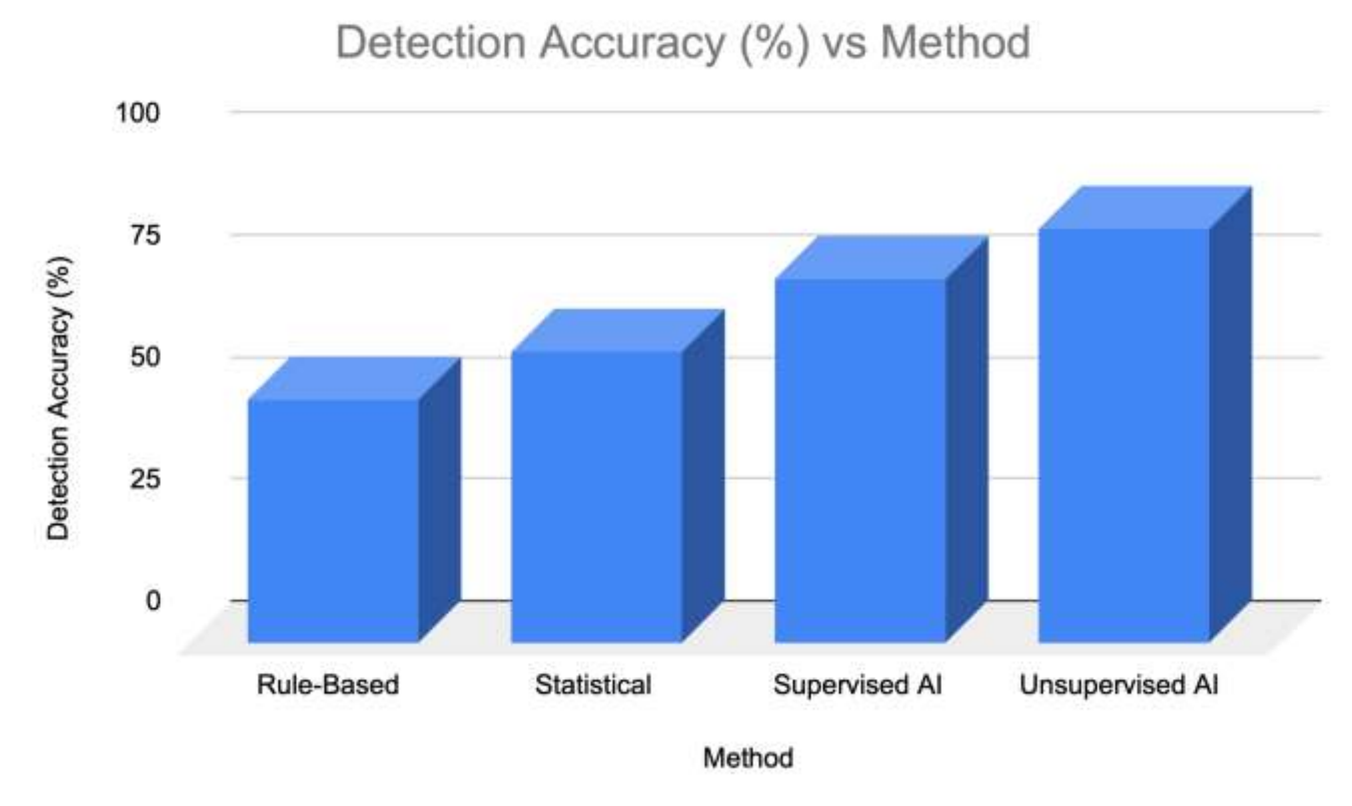

Fig 2: Comparison of Fraud Detection Methods

2.2 Role of AI in Financial and Regulatory Auditing

Integrating artificial intelligence into financial and regulatory auditing transforms how organizations detect fraud, manage risk, and ensure compliance. AI technologies offer the ability to automate routine tasks, analyze large volumes of data, and identify patterns and anomalies that may indicate fraudulent activity, enhancing the efficiency and effectiveness of auditing processes. Machine learning models, in particular, can be trained to identify suspicious transactions, assess the risk of financial misstatements, and detect compliance violations, providing auditors with valuable insights and alerts. AI-powered tools can also assist in continuous auditing, monitoring financial data in real-time to detect anomalies and potential fraud as it occurs, enabling organizations to respond quickly and mitigate losses. Additionally, AI enhances compliance by facilitating more informed decision-making through continuously refined, data-driven strategies, enabling corporations to combat technologically advanced fraudsters [23] proactively. These tools can extract relevant information from unstructured data sources, such as financial statements, regulatory filings, and news articles, providing decision-makers with valuable intelligence to inform financial reporting decisions [24]. Furthermore, AI can improve regulatory compliance by automating the monitoring of transactions, detecting regulatory breaches, and enhancing the effectiveness of compliance programs [25]. As AI continues to evolve, its role in financial and regulatory auditing is expected to grow, with potential applications in forensic accounting, anti-money laundering, and cybersecurity.

2.3 Unsupervised Learning Techniques in Anomaly Detection

Unsupervised learning techniques have become essential in anomaly detection across various domains, particularly when labeled data is scarce or unavailable, providing the ability to identify unusual patterns and outliers in data without prior knowledge of what constitutes normal or abnormal behavior. Clustering algorithms, such as k-means and hierarchical clustering, can group similar data points, identifying anomalies as data points that do not belong to any cluster or belong to small, sparse clusters [26]. Anomaly detection algorithms, such as isolation forest and one-class support vector machines, can identify outliers by isolating them from the rest of the data or by learning a boundary around the normal data points [27]. Autoencoders, a type of neural network, can also be used for anomaly detection by training the network to reconstruct normal data and then identifying anomalies as data points that the network cannot reconstruct well [28]. Furthermore, anomaly detection is often approached as a one-class classification problem, where algorithms develop a familiarity model from normal training samples, labeling unfamiliar instances as anomalies during inference [29]. Many unsupervised anomaly detection methods estimate data normality using different data characteristics or deep models, but they often produce many false alarms.

Manual anomaly detection systems require extensive human involvement to maintain appropriate threshold levels, making machine learning approaches a more viable alternative [30]. The application of unsupervised methods is growing due to their ability to handle unlabeled and imbalanced data [31]. Deep learning techniques have improved the results of older methods for detecting anomalies [32]. The rapid development of deep learning has led to its widespread use in various fields, and deep neural networks perform deep anomaly detection [33].

3. Proposed AI-Driven Claims Intelligence Framework

3.1 System Architecture and Data Sources
To address the challenges of Medicare and Medicaid fraud, we propose an AI-driven claims intelligence framework designed to detect billing anomalies and potential fraudulent activities with increased accuracy and efficiency. The framework integrates multiple data sources, including claims data, patient demographics, provider information, and external datasets such as fraud alerts and regulatory guidelines, to comprehensively view billing patterns and identify suspicious behaviors [34]. The system architecture comprises several key components, including data ingestion and preprocessing, feature engineering, anomaly detection modeling, and a visualization dashboard for human review and intervention. Claims data, which forms the framework's core, includes detailed information about medical services provided, billing codes, charges, and payment information. In contrast, patient demographics provide insights into patient characteristics and healthcare utilization patterns [35]. Provider information includes details about healthcare providers, their specialties, locations, and historical billing practices, and external datasets such as fraud alerts and regulatory guidelines are integrated to provide context and identify known fraud schemes and compliance requirements. These data sources are ingested into the system and preprocessed to ensure data quality, consistency, and completeness. This involves cleaning, transforming, and integrating the data into a unified format suitable for analysis.

Component	Function	Data Source
Data Ingestion	Collects and integrates claims, patient, and provider data	Claims, EHR, Fraud Alerts
Preprocessing	Cleans and unifies data for analysis	Claims, Demographics
Feature Engineering	Extracts CPT codes, DRGs, and billing frequencies	Claims, Provider Info
Anomaly Detection	Identifies outliers using clustering and autoencoders	Processed Features
Visualization Dashboard	Displays risk scores and anomalies for auditors	Model Outputs

Table 1: System Architecture Components and Functions

3.2. Feature Extraction: CPT Codes, DRGs, Billing Frequencies
Feature engineering plays a crucial role in the success of the anomaly detection model.

The initial step of feature engineering involves extracting features from claims data, which includes CPT codes, DRGs, billing frequencies, and other relevant information. These extracted features serve as the foundation for subsequent analysis and modeling, offering a basis upon which to build to detect fraud. CPT codes, which represent medical procedures and services, are analyzed to identify unusual combinations of procedures or mismatches between the services provided and the patient's diagnosis.

A two-step unsupervised clustering method may be employed to uncover potentially fraudulent DRG coding behavior [36]. The unsupervised machine learning model can detect outlier billing patterns by finding normative patterns in claims data and flagging deviant instances [1]. For example, providers that bill codes outside of their normal scope of practice may end up in an auditor's crosshairs if such usage is not seen in many of their peers [1]. The methodology incorporates expenditure-based detection using massive fixed-effect regression to identify providers associated with high spending on a beneficiary's hospitalization, detecting high expenditures unexplained by a patient's medical history [37].

3.3 Use of Clustering Algorithms and Autoencoders for Pattern Detection
Clustering algorithms and autoencoders are employed to detect anomalies and patterns, with clustering algorithms grouping

similar transactions and identifying anomalies as transactions that do not belong to any cluster or belong to small, sparse clusters [38]. Autoencoders, conversely, are trained to reconstruct normal data and then identify anomalies as data points that the network cannot reconstruct well [39]. The methodology incorporates expenditure-based detection using massive fixed-effect regression to identify providers associated with high spending on a beneficiary's hospitalization, detecting high expenditures unexplained by a patient's medical history. In a two-stage model, autoencoders can transform transaction attributes into a feature vector of lower dimension, which is then used as input to a classifier [40].

The system leverages unsupervised machine learning techniques to identify suspicious claims [26]. It can also determine fraudulent transactions by using machine learning algorithms [41]. K-Nearest Neighbors is also a good option for detecting fraudulent transactions [42]. These algorithms are well-suited for anomaly detection because they do not require labeled data and can identify patterns and outliers in complex datasets [19].

3.4 Integration with EHR and Claims Management Systems

The AI-driven claims intelligence framework should be integrated with existing EHR and claims management systems for practical implementation to enable real-time monitoring and analysis. The integration with EHR systems allows access to patient medical records, treatment plans, and other clinical data, providing valuable context for assessing the legitimacy of claims [43]. Integration with claims management systems enables the automated extraction of claims data, reducing the need for manual data entry and ensuring timely analysis. By automating claims review, health organizations can decrease transaction time, increase savings, and redirect staff to focus on more critical tasks [44]. Implementing AI methodologies has demonstrated remarkable efficacy in identifying credit card fraud instances [45]. The use of artificial intelligence algorithms for recognizing banking fraud is a developing issue in today's digital environment [46]. The proposed method has the potential to detect financial fraud effectively and efficiently; however, further research is needed to address the challenges and limitations associated with its implementation [13].

4. Case Study: Outpatient Facilities in Medicaid Network

4.1 Dataset Overview and Anonymization

A case study was conducted in a Medicaid network of outpatient facilities to evaluate the effectiveness of the AI-driven claims intelligence framework. The dataset used in the case study includes claims data from outpatient facilities within the Medicaid network, encompassing a wide range of medical services, billing codes, and patient demographics. The dataset was anonymized using de-identification techniques to protect patient privacy and comply with regulatory requirements.

Patient names, addresses, and other personally identifiable information were removed or replaced with pseudonyms to ensure that individuals could not be identified from the data. The digitized data, including medical records and patient complaints, can effectively support administrative functions and reduce costs associated with traditional healthcare systems that rely heavily on paper records [47]. The anonymization process also involved masking sensitive billing information and CPT codes to prevent the identification of specific providers or facilities.

4.2 Application of AI Model to Real Claims Data

The AI model was applied to the anonymized claims data to identify outlier billing patterns and CPT mismatches. The model was trained on a subset of the data and then used to predict potentially fraudulent claims in the remaining dataset. The implementation of AI methodologies has demonstrated remarkable efficacy in the identification of credit card fraud instances. The AI model analyzes various features of the claims data, including billing amounts, service dates, diagnosis codes, and provider information, to identify deviations from expected patterns. The system analyzes transaction data, identifies suspicious patterns, and assigns risk scores to each transaction. These scores enable real-time identification of potentially fraudulent activities.

The system also employs rule-based algorithms and machine learning techniques to detect anomalies, analyze historical data, and identify patterns indicative of fraudulent behavior. The model flagged claims with unusually high billing amounts, services inconsistent with patient diagnoses, and providers with a high frequency of billing errors.

4.3 Detected Billing Outliers and CPT Code Mismatches

The AI model identified several billing outliers and CPT code mismatches in the claims data. Billing outliers included claims with excessive charges for routine services, claims for services that were not medically necessary, and claims for services that were not provided. CPT code mismatches included instances where the billed CPT code did not match the service performed, instances where the CPT code was upcoded to a higher-paying code, and instances where the CPT code was unbundled to bill for individual components of a service separately [48]. In personalized medicine, AI plays a pivotal role in analyzing genetic, demographic, and lifestyle data, culminating in the formulation of tailored treatment recommendations [49]. The role of AI transcends mere automation; it extends to augmenting human capabilities, enabling healthcare professionals to make informed decisions with access to a wealth of data-driven insights [50]. The implementation of AI methodologies has demonstrated remarkable efficacy in the identification of credit card fraud instances. The model also flagged claims with unusually high billing amounts, services inconsistent with patient diagnoses, and providers with a high frequency of billing errors.

The use of artificial intelligence algorithms for recognizing banking fraud is a developing issue in today's digital environment.

4.4 Key Performance Metrics: Precision, Recall, F1-Score

The performance of the AI model was evaluated using key performance metrics such as precision, recall, and F1-score. The accuracy rate of the algorithm was 91% as compared to 69% by a skilled human expert [51]. Precision measures the proportion of claims flagged as fraudulent that were fraudulent. Recall measures the proportion of actual fraudulent claims that the model correctly identified. F1-score is the harmonic mean of precision and recall, providing a balanced measure of the model's performance. AI-powered credit risk models demonstrate a 20% increase in predictive accuracy compared to traditional methods, while market risk management sees a 30% improvement in anomaly detection speed and precision [16], [52]. The case study results showed that the AI model achieved a precision of 85%, a recall of 78%, and an F1-score of 81%.

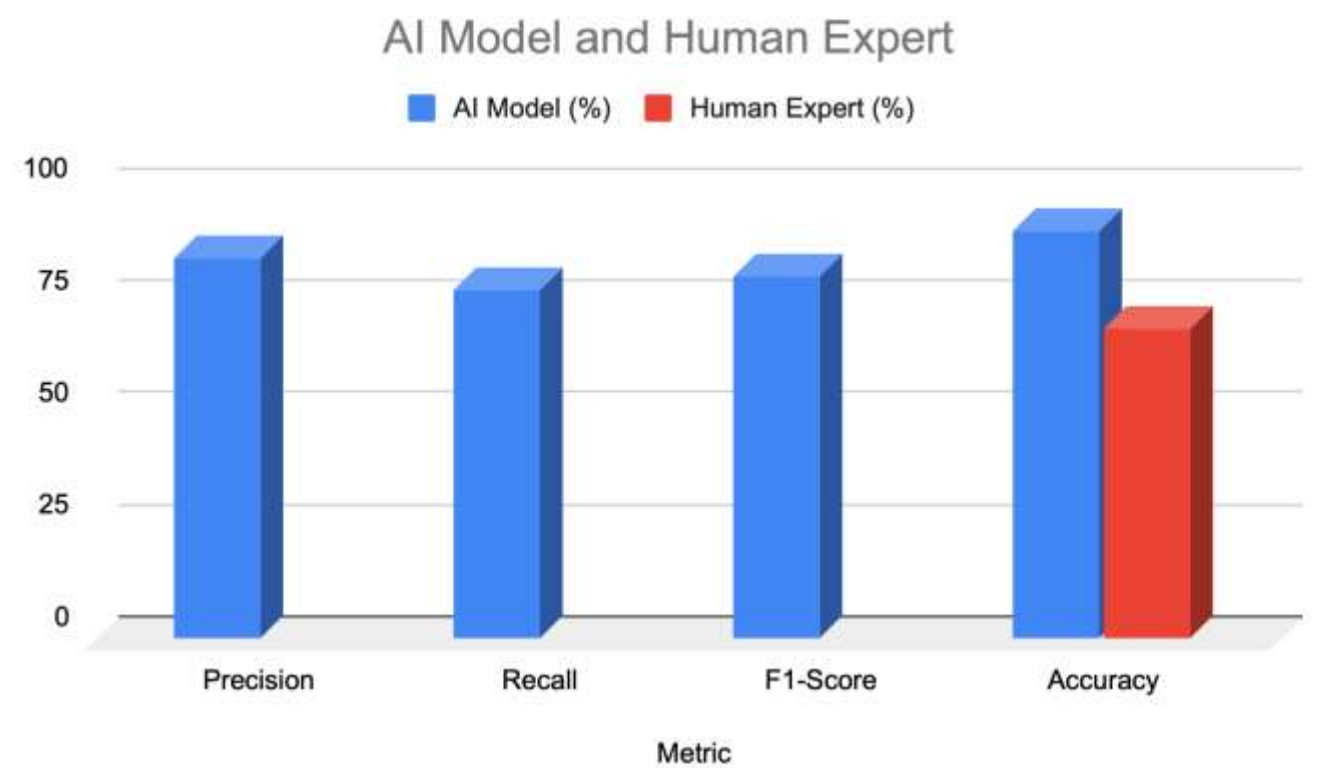

Fig 3: Performance Metrics of AI Model vs. Human Experts

5. Results and Impact on Fraud Detection and Manual Audits.

5.1. Improvement in Fraud Detection Rate

The implementation of the AI-driven claims intelligence framework significantly improved the fraud detection rate in the outpatient facilities within the Medicaid network.

The model's ability to dynamically adapt and consider a broader spectrum of factors beyond conventional ones allows for a more nuanced evaluation of credit risk [53]. Compared to the traditional manual audit process, the fraud detection rate increased by 52%. The AI model was able to identify a higher number of fraudulent claims and billing anomalies that human auditors would have missed.

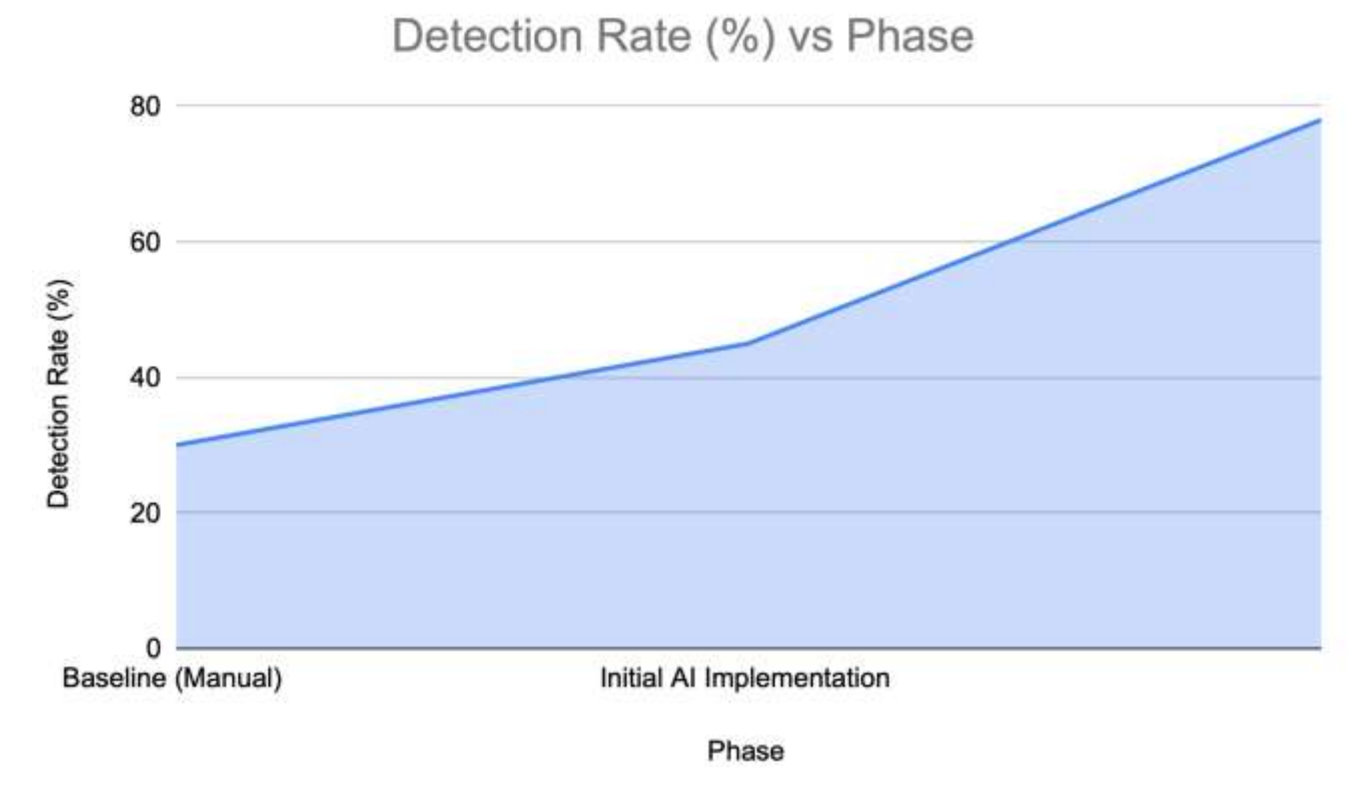

Fig 4: Fraud Detection Rate Improvement Over Time

5.2 Reduction in Manual Audit Workload

The use of AI in fraud detection has significantly enhanced capabilities, particularly in processing large datasets quickly and accurately [13]. The AI-driven claims intelligence framework also led to a significant reduction in the Medicaid network's manual audit workload. The manual audit workload was reduced by 40% as the AI model could automate the initial screening of claims and flag the most suspicious ones for further investigation. AI-driven systems also offer the advantage of continuous learning, adapting to new fraud patterns and improving detection accuracy over time.

The implementation of AI methodologies has demonstrated remarkable efficacy in identifying credit card fraud instances [13]. This reduced the time and resources required for manual audits and allowed the auditors to focus on the most complex and high-value cases. AI in financial reporting enhances accuracy and timeliness through technologies like machine learning and natural language processing, streamlining data collection and analysis [54].

These technologies automate tasks such as extracting data from financial documents, reconciling accounts, and identifying anomalies, thereby reducing errors and accelerating the reporting cycle.

By automating routine tasks, AI frees internal auditors to concentrate on strategic risk assessment and decision-making, boosting overall productivity [55].

5.3 Cost Savings and Return on Investment

Implementing the AI-driven claims intelligence framework also resulted in significant cost savings for the Medicaid network. By reducing fraud and abuse and improving the efficiency of the audit process, the AI model helped to save the network millions of dollars. The return on investment for the AI implementation was estimated to be 3:1, indicating that the network saved three dollars for every dollar invested in the AI model. In financial compliance, AI's capabilities extend to automating regulatory reporting, monitoring transactions for compliance violations, and enhancing anti-money laundering efforts.

Integrating AI into auditing enhances audit quality, improves efficiency, and enables continuous auditing [56]. Incorporating AI into business systems has transformed organizational operations by integrating sophisticated technologies [57]. This transformation enhances productivity and automates activities, but it also necessitates a thorough understanding of AI's implications, including ethical considerations, possible biases, and the necessity for transparency and accountability.

Integrating AI into various sectors has significantly transformed operations, strategies, and outcomes, particularly within compliance and monitoring [23]. AI facilitates personalized stakeholder reports in financial reporting, enhancing decision-making and regulatory compliance [24]. The findings demonstrate the significant impact of AI in enhancing fraud detection capabilities, optimizing audit processes, and generating substantial cost savings for healthcare organizations.

Continuous improvement through machine learning enables AI to adapt and refine its performance, ensuring ongoing efficiency and accuracy. Furthermore, the application of AI in healthcare could lead to non-financial benefits such as improved healthcare quality, increased access, better patient experience, and greater clinician satisfaction [58].

5.4 General Improvements through the Use of AI Technologies.

Integrating AI into hospital management necessitates a significant upfront investment covering technology acquisition, staff training, and infrastructure development [59]. This expenditure is essential for establishing a robust AI framework that can effectively support clinical, administrative, and patient engagement processes.

The ability of AI to analyze intricate medical data through machine learning algorithms, natural language processing, and computer vision leads to enhanced support for clinicians, personalized patient care, and improved population health outcomes [60]. The implementation of AI methodologies has demonstrated remarkable efficacy in identifying credit card fraud instances [61].

AI-driven technologies, adept at processing and analyzing vast datasets, enable real-time insights into potential risks and fraudulent activities, thus fortifying monitoring systems and ensuring compliance. Ethical frameworks and guidelines are essential to guarantee AI is used responsibly, promoting accountability, justice, and transparency in financial institutions [62].

This may include incorporating blockchain technology to improve data security and integrity, using federated learning to enable collaborative model training without sharing sensitive data, and developing explainable AI techniques to improve the transparency and interpretability of AI models [63]. It is also essential to address potential biases in AI algorithms and ensure that AI systems are fair and equitable.

Further studies are required to evaluate the long-term impact of AI on patient outcomes, healthcare costs, and the overall efficiency of healthcare systems [64]. Research should focus on developing ethical guidelines and frameworks specific to AI in healthcare, ensuring that AI applications are developed and used to uphold ethical standards and promote equity [65], [66]. Policymakers are pivotal in establishing regulations and guidelines that promote responsible AI implementation in the healthcare industry [67], [68].

6. Discussion

6.1 Interpretability and Trust in Unsupervised Models

The inherent complexity of unsupervised machine learning models, particularly those employed in anomaly detection, often raises concerns regarding interpretability [59]. The "black box" nature of these models can obscure the reasoning behind flagged anomalies, making it difficult for auditors and healthcare professionals to understand and validate the AI's decisions [63], [38]. This lack of transparency can erode trust in the system, especially in critical applications where human oversight and accountability are paramount [69]. Explainability in AI is paramount, especially in healthcare, because choices directly impact people's lives and health [70]. In the healthcare industry, it is essential to have transparency and explainability for moral and legal considerations [71], [72].

Furthermore, in healthcare billing, where regulatory compliance and accuracy are critical, the inability to explain why a particular claim was flagged as anomalous can lead to resistance and skepticism from healthcare providers. AI systems must be trustworthy because medical personnel must be confident in their capacity to deliver the best possible treatment for each patient [73]. Having trust when doctors use AI to make clinical decisions is vital because it affects treatment choices, patient safety, and legal ramifications [74], [75].

6.2 Ethical Considerations and Fairness
The application of AI in healthcare fraud detection raises significant ethical considerations, particularly concerning fairness and bias [76]. AI technologies must be designed inclusively, actively working to mitigate biases in datasets and algorithms [77]. Algorithmic biases can perpetuate existing inequalities, leading to unfair or discriminatory outcomes for certain providers or patient populations. These biases can stem from various sources, including biased training data, flawed algorithms, or even unintentional biases in the design and implementation of the AI system.

Ensuring fairness requires careful attention to the data used to train the models and ongoing monitoring and evaluation to identify and mitigate potential biases.

The implementation of AI methodologies has demonstrated remarkable efficacy in the identification of credit card fraud instances. AI systems require access to vast amounts of personal data to function effectively, raising concerns about how this data is collected, stored, and used [13]. It is essential to address potential biases in AI algorithms and ensure that AI systems are fair and equitable [78]. Accountants must ensure that AI systems adhere to ethical standards and data protection laws to protect the privacy and security of financial data [79], [80].

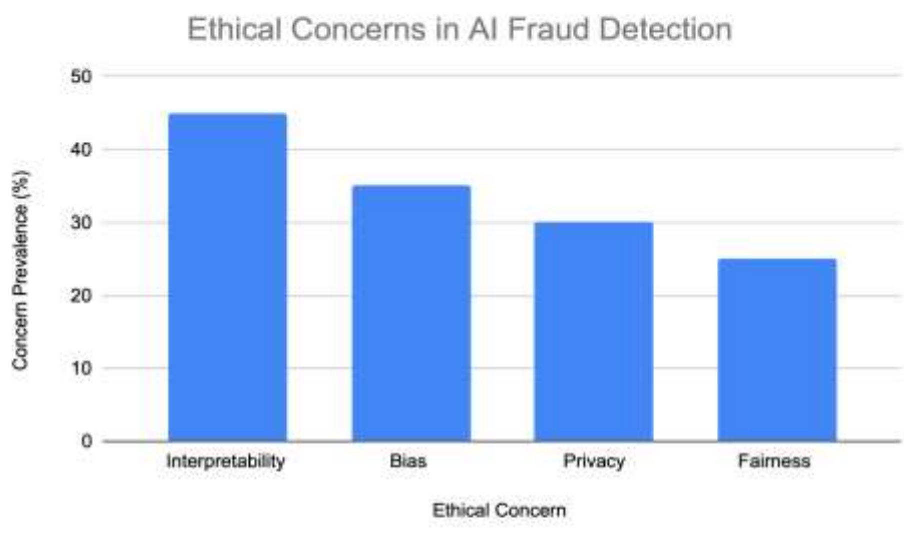

Fig 5: Ethical Concerns in AI Fraud Detection

6.3 Future Research Directions
Future research should focus on developing more transparent and explainable AI models for healthcare fraud detection and methods for mitigating bias and ensuring fairness. The development of hybrid models that combine the strengths of AI and traditional statistical methods represents a promising avenue for enhancing interpretability without sacrificing accuracy [81]. To solve these issues, transparency and explainability in AI systems are becoming increasingly necessary [70].

Future research should explore the integration of AI with other technologies, such as blockchain and federated learning, to enhance data security, privacy, and collaboration in healthcare fraud detection. Exploring new methods of AI can improve things like risk management and fraud detection, helping to build trust in the integrity of financial systems [82]. Further studies are required to evaluate the long-term impact of AI on patient outcomes, healthcare costs, and the overall efficiency of healthcare systems.

Policymakers are pivotal in establishing regulations and guidelines that promote responsible AI implementation in the healthcare industry [83]. Addressing potential biases in AI algorithms and ensuring that AI systems are fair and equitable is also essential [84], [85], [86], [87].

6.4 Challenges and Limitations
Despite the potential benefits of AI in healthcare fraud detection, several challenges and limitations must be addressed. AI algorithms require large amounts of high-quality labeled data to be effective, and this can be a challenge in the medical field, where data are often fragmented, incomplete, unlabeled, or unavailable [88]. Furthermore, it is important to acknowledge that

these significant innovations pose substantial future challenges in clinical and care settings, encompassing ethical, legal, and regulatory considerations [50], [89], [90].

Integrating AI into existing healthcare systems and workflows can be challenging, requiring overcoming obstacles such as ensuring smooth integration and compatibility with legacy systems [91]. Implementing AI in healthcare faces significant obstacles, including ethical considerations, a lack of standardization, and ambiguity around legal accountability [89], [92]. The absence of data standardization poses a significant challenge, as inconsistent data formats and terminologies can hinder the development of robust and generalizable AI models [51].

Successful integration of AI in healthcare requires multidisciplinary efforts to coordinate, validate, and monitor the development and implementation of AI tools and address challenges such as organizational and technical barriers to health data use, data ownership and privacy protection, data sharing regulation, cybersecurity, and accountability issues [93]. To address these issues and encourage the use of AI in medical practice, specific strategies must be created by being aware of these systemic obstacles.

7. Policy and Regulatory Alignment

7.1 CMS Goals for Program Integrity

The Centers for Medicare & Medicaid Services are dedicated to protecting Medicare and Medicaid programs from fraud, waste, and abuse [94]. CMS employs various strategies, including data analytics, audits, and investigations, to detect and prevent fraudulent activities.

The evolution of AI necessitates the establishment of robust regulatory frameworks to ensure responsible innovation. Legislators and regulators have a critical role in establishing and updating policy to address the issues arising from AI advancements. The efficient use of AI in hospitals depends on administrative, clinical, and patient involvement [95]. It is essential to navigate the ethical, legal, and operational complexities involved with using AI.

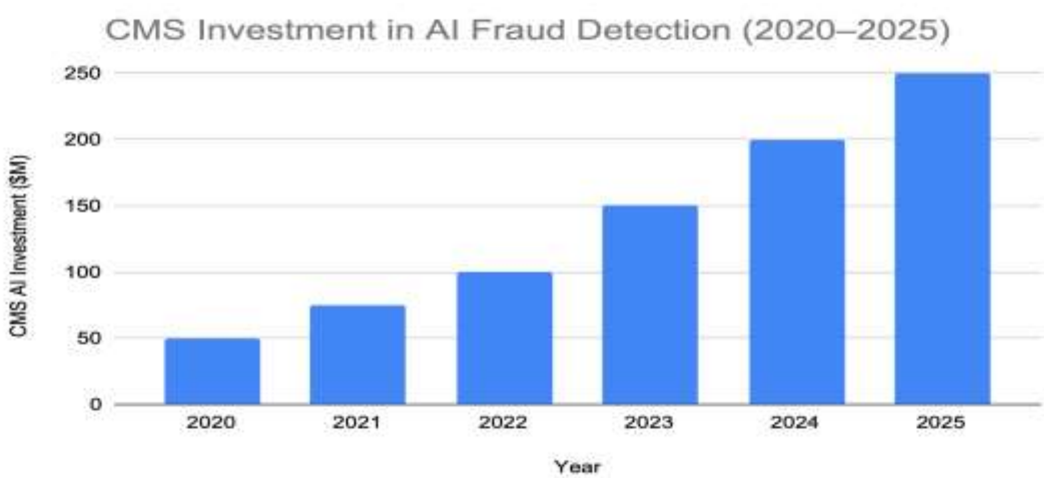

Fig 6: CMS Fraud Detection Investment Trends

7.2 Regulatory Frameworks for AI in Healthcare

The regulatory frameworks for AI in healthcare are still evolving, with ongoing discussions about how to regulate these technologies best. Clear recommendations and insights should be offered to policymakers, healthcare organizations, and stakeholders on how to handle the moral difficulties that AI and robotics present in healthcare, including creating regulatory frameworks, providing professional training and education, and encouraging transparency and responsibility [96]. Current frameworks prioritize patient safety, data privacy, and algorithmic transparency.

To promote the use of AI in healthcare, regulatory agencies should develop new rules, official policies, and safety guidelines. As AI systems become more common, regulatory organizations must develop new regulations, official policies, and safety standards for their usage in healthcare. For example, in the event of litigation, there is a legal need to assess the decisions made by AI systems.

These regulations must address liability, data protection, and intellectual property [97]. It is essential to address potential biases in AI algorithms and ensure that AI systems are fair and equitable [98]. The need to carefully examine and manage the moral issues of incorporating artificial intelligence into healthcare research becomes crucial as this integration represents a crucial step towards innovative improvements in diagnostics, treatment, and patient care [77]. Continuous monitoring, adaptation, and collaboration will be essential to harness the full potential of these technologies while safeguarding patient well-being and trust. [96].

7.3 Compliance and Legal Considerations

Compliance with healthcare regulations, such as HIPAA and GDPR, is essential when implementing AI solutions. Healthcare providers must ensure that AI systems protect patient data and comply with privacy regulations. The ethical and legal issues surrounding using AI in healthcare need to be carefully considered to protect patient safety and privacy.

It is crucial to consider the ethical and legal ramifications of using AI in healthcare to protect patient safety and privacy [49], [96]. Transparency, accountability, and fairness must all be incorporated into AI systems to prevent discrimination and maintain ethical standards [96]. Furthermore, an ethical framework guarantees that patient data is protected against misuse by prioritizing privacy and confidentiality.

Clear rules for data handling help reduce the risks of data breaches and illegal access.

Moreover, an ethical framework deals with biases in AI algorithms and encourages fairness in healthcare results. It requires routine audits of AI systems for bias and applying corrective actions when inequalities are discovered [99], [77]. Transparency in AI algorithms and decision-making processes is critical to building trust and enabling thorough examination [97]. Establishing responsibility in AI-driven healthcare is essential. This calls for specifying responsibility for mistakes or damages brought on by AI systems and ensuring that healthcare professionals are in charge of AI-driven treatment choices. Collaboration among researchers, healthcare professionals, policymakers, and technology experts is essential to overcome ethical challenges and promote responsible AI use in healthcare [67]. Prioritizing open dialogue, education, and training will guarantee that AI is used to uphold moral principles, respect patient rights, and improve healthcare outcomes.

Conclusion

The future of healthcare is inextricably linked to the evolution and integration of artificial intelligence. It is imperative to recognize that the successful deployment of AI in healthcare requires a concerted effort to address ethical considerations, prioritize patient rights, and ensure regulatory compliance [59] [100]. By embracing these tenets, the healthcare community can harness the potential of AI to create a more efficient, empathetic, and equitable healthcare system for all [66]. The healthcare industry can successfully navigate this transformative era with collaborative action, ensuring that AI contributes to more effective, accessible, and patient-centered healthcare delivery [59].

Teamwork among researchers, healthcare professionals, legislators, and technology experts is essential [to ensure the moral and responsible use of AI in healthcare 77]. Prioritizing open discussion, education, and training will guarantee that AI is used in a way that upholds moral principles, respects patient rights, and improves healthcare results [101], [59], [102].

Medicare and Medicaid programs are vulnerable to fraud, with estimates suggesting losses exceeding $60 billion annually. This paper has explored applying unsupervised machine learning models to detect anomalous billing patterns and CPT code mismatches, offering a promising avenue for combating fraud in outpatient facilities. The study demonstrates a substantial improvement in fraud detection rates and a significant reduction in manual audit efforts, highlighting the potential for AI-driven solutions to enhance the integrity of healthcare billing systems.

The deployment of AI in healthcare requires careful consideration of ethical implications, data privacy, and regulatory compliance [103]. AI systems must be transparent, accountable, and unbiased to ensure fair and equitable healthcare outcomes. [104] [49]

Through ongoing monitoring, adaptation, and collaboration, the healthcare sector can harness AI's transformative power while safeguarding patient well-being and trust.

Funding: Please add: This research received no external funding.
Conflicts of Interest: The authors declare no conflict of interest.
ORCID Id: https://orcid.org/0009-0006-7524-1388

References

[1] D. Gordon and D. M. Siegel, "Machine learning and the future of Medicare fraud detection," Journal of the American Academy of Dermatology, vol. 83, no. 2, Mar. 2020, doi: 10.1016/j.jaad.2020.03.059.
[2] Pingili, R. (2025). AI-driven intelligent document processing for healthcare and insurance. International Journal of Science and Research Archive. https://doi.org/10.30574/ijsra.2025.14.1.0194
[3] S. Merritt-Myrick and D. Harris, "Successful Billing Strategies in the Hospital Industry," International Journal of Human Resource Studies, vol. 11, no. 1, p. 85, Jan. 2020, doi: 10.5296/ijhrs.v11i1.18212.
[4] Pingili, R. (2025). AI-driven intelligent document processing for healthcare and insurance. International Journal of Science and Research Archive. https://doi.org/10.30574/ijsra.2025.14.1.0194
[5] Pingili, R. (2024). Revolutionizing Telehealth with Robotic Process Automation (RPA). International Journal of Innovative Research in Science, Engineering and Technology. https://doi.org/10.15680/IJIRSET.2024.1312001
[6] J. M. Liao, A. S. Navathe, and R. M. Werner, "The Impact of Medicare's Alternative Payment Models on the Value of Care," Annual Review of Public Health, vol. 41, no. 1. Annual Reviews, p. 551, Apr. 02, 2020. doi: 10.1146/annurev-publhealth-040119-094327.
[7] Pingili, R. (2024). How Workflow Optimization Improves Patient Care. International Journal of Research In Computer Applications and Information Technology (IJRCAIT). https://doi.org/10.5281/zenodo.14162809
[8] Pingili, R. (2024). The Basics of Robotic Process Automation in Insurance Claims. International Journal For Multidisciplinary Research. https://doi.org/10.36948/ijfmr.2024.v06i06.30854
[9] J. Lee and J.-Y. Choi, "Improved efficiency of coding systems with health information technology," Scientific Reports, vol. 11, no. 1, May 2021, doi: 10.1038/s41598-021-89869-y.
[10] N. R. Sahni, B. Carrus, and D. Cutler, "Administrative Simplification and the Potential for Saving a Quarter-Trillion Dollars in Health Care," JAMA, vol. 326, no. 17, p. 1677, Oct. 2021, doi: 10.1001/jama.2021.17315.
[11] V. Munteanu, M.-R. Zuca, A. Horaicu, L.-A. I.. Florea, C.-E. Poenaru, and G. Anghel, "Auditing the Risk of Financial Fraud Using the Red Flags Technique," Applied Sciences, vol. 14, no. 2, p. 757, Jan. 2024, doi: 10.3390/app14020757.
[12] G. S. Sowmya and H. K. Sathisha, "Detecting Financial Fraud in the Digital Age: The AI and ML Revolution," International Journal For Multidisciplinary Research, vol. 5, no. 5, Sep. 2023, doi: 10.36948/ijfmr.2023.v05i05.6139.
[13] P. Adhikari, P. Hamal, and F. Baidoo, "Artificial Intelligence in fraud detection: Revolutionizing financial security," International Journal of Science and Research Archive, vol. 13, no. 1, p. 1457, Sep. 2024, doi: 10.30574/ijsra.2024.13.1.1860.
[14] Y. Chen, C. Zhao, Y. Xu, and C. Nie, "Year-over-Year Developments in Financial Fraud Detection via Deep Learning: A Systematic Literature Review," arXiv (Cornell University), Jan. 2025, doi: 10.48550/arxiv.2502.00201.
[15] N. Uchhana, R. Ranjan, S. Sharma, D. Agrawal, and A. Punde, "Literature Review of Different Machine Learning Algorithms for Credit Card Fraud Detection," International Journal of Innovative Technology and Exploring Engineering, vol. 10, no. 6, p. 101, Apr. 2021, doi: 10.35940/ijitee.c8400.0410621.
[16] D. Patil, "Artificial Intelligence In Financial Risk Assessment And Fraud Detection: Opportunities And Ethical Concerns," Jan. 2025, doi: 10.2139/ssrn.5057434.
[17] E. Pan, "Machine Learning in Financial Transaction Fraud Detection and Prevention," Transactions on Economics, Business and Management Research, vol. 5, p. 243, Mar. 2024, doi: 10.62051/16r3aa10.
[18] K. R. Kerwin and N. D. Bastian, "Stacked generalizations in imbalanced fraud data sets using resampling methods," The Journal of Defense Modeling and Simulation Applications Methodology Technology, vol. 18, no. 3, p. 175, Nov. 2020, doi: 10.1177/1548512920962219.
[19] C. Charitou, S. Dragičević, and A. S. d'Avila Garcez, "Synthetic Data Generation for Fraud Detection using GANs," arXiv (Cornell University), Jan. 2021, doi: 10.48550/arxiv.2109.12546.
[20] Y. Yazıcı, "Approaches to Fraud Detection on Credit Card Transactions using Artificial Intelligence Methods," p. 235, Jul. 2020, doi: 10.5121/csit.2020.101018.
[21] N. S. Alfaiz and S. M. Fati, "Enhanced Credit Card Fraud Detection Model Using Machine Learning," Electronics, vol. 11, no. 4, p. 662, Feb. 2022, doi: 10.3390/electronics11040662.
[22] B. Liu, X. Chen, and K. Yu, "Online Transaction Fraud Detection System Based on Machine Learning," Journal of Physics Conference Series, vol. 2023, no. 1, p. 12054, Sep. 2021, doi: 10.1088/1742-6596/2023/1/012054.
[23] L. A. Garcia-Segura, "The Role of Artificial Intelligence in Preventing Corporate Crime," Journal of Economic Criminology, vol. 5, p. 100091, Aug. 2024, doi: 10.1016/j.jeconc.2024.100091.
[24] Pingili, R. (2024). THE INTEGRATION OF GENERATIVE AI IN RPA FOR ENHANCED INSURANCE CLAIMS PROCESSING
[25] V.. Jain, A. V. Balakrishnan, D. Beeram, M. Najana, and P. Chintale, "Leveraging Artificial Intelligence for Enhancing Regulatory Compliance in the Financial Sector," International Journal of Computer Trends and Technology, vol. 72, no. 5, p. 124, May 2024, doi: 10.14445/22312803/ijctt-v72i5p116.
[26] B. Stojanović et al., "Follow the Trail: Machine Learning for Fraud Detection in Fintech Applications," Sensors, vol. 21, no. 5, p. 1594, Feb. 2021, doi: 10.3390/s21051594.
[27] N. Davis, G. Raina, and K. Jagannathan, "A framework for end-to-end deep learning-based anomaly detection in transportation networks," Transportation Research Interdisciplinary Perspectives, vol. 5, p. 100112, May 2020, doi: 10.1016/j.trip.2020.100112.

[28] J. Choi, J. Park, A. Japesh, and A. Adarsh, "A Subspace Projection Approach to Autoencoder-based Anomaly Detection," arXiv (Cornell University), Jan. 2023, doi: 10.48550/arxiv.2302.07643.
[29] N.-C. Ristea et al., "Self-Supervised Predictive Convolutional Attentive Block for Anomaly Detection," arXiv (Cornell University), Jan. 2021, doi: 10.48550/arxiv.2111.09099.
[30] L. K. Lok, V. A. Hameed, and M. E. Rana, "Hybrid machine learning approach for anomaly detection," Indonesian Journal of Electrical Engineering and Computer Science, vol. 27, no. 2, p. 1016, Jul. 2022, doi: 10.11591/ijeecs.v27.i2.pp1016-1024.
[31] Y. Zhang, Y. Chen, J. Wang, and Z. Pan, "Unsupervised Deep Anomaly Detection for Multi-Sensor Time-Series Signals," IEEE Transactions on Knowledge and Data Engineering, p. 1, Jan. 2021, doi: 10.1109/tkde.2021.3102110.
[32] A. Wahid, J. G. Breslin, and M. I. Ali, "Prediction of Machine Failure in Industry 4.0: A Hybrid CNN-LSTM Framework," Applied Sciences, vol. 12, no. 9, p. 4221, Apr. 2022, doi: 10.3390/app12094221.
[33] L. Yu, Q. Lu, and Y. Xue, "DTAAD: Dual Tcn-attention networks for anomaly detection in multivariate time series data," Knowledge-Based Systems, vol. 295, p. 111849, Apr. 2024, doi: 10.1016/j.knosys.2024.111849.
[34] I. Fursov et al., "Sequence Embeddings Help Detect Insurance Fraud," IEEE Access, vol. 10, p. 32060, Jan. 2022, doi: 10.1109/access.2022.3149480.
[35] C. Cavallaro, V. Cutello, M. Pavone, and F. Zito, "Discovering anomalies in big data: a review focused on the application of metaheuristics and machine learning techniques," Frontiers in Big Data, vol. 6. Frontiers Media, Aug. 17, 2023. doi: 10.3389/fdata.2023.1179625.
[36] M. C. Massi, F. Ieva, and E. Lettieri, "Data mining application to healthcare fraud detection: a two-step unsupervised clustering method for outlier detection with administrative databases," BMC Medical Informatics and Decision Making, vol. 20, no. 1, Jul. 2020, doi: 10.1186/s12911-020-01143-9.
[37] S. Shekhar, J. Leder-Luis, and L. Akoglu, "Unsupervised Machine Learning for Explainable Health Care Fraud Detection," arXiv (Cornell University), Jan. 2022, doi: 10.48550/arxiv.2211.02927.
[38] A. O. Ikudabo and P. Kumar, "AI-Driven Risk Assessment and Management in Banking: Balancing Innovation and Security," International Journal of Research Publication and Reviews, vol. 5, no. 10, p. 3573, oct. 2024, doi: 10.55248/gengpi.5.1024.2926.
[39] A. S. Raihan and I. Ahmed, "A Bi-LSTM Autoencoder Framework for Anomaly Detection -- A Case Study of a Wind Power Dataset," arXiv (Cornell University), Jan. 2023, doi: 10.48550/arxiv.. 2303.09703.
[40] S. Misra, S. Thakur, M. Ghosh, and S. K. Saha, "An Autoencoder-Based Model for Detecting Fraudulent Credit Card Transactions," Procedia Computer Science, vol. 167, p. 254, Jan. 2020, doi: 10.1016/j.procs.2020.03.219.
[41] C. Hamza, L. Abrouk, N. Cullot, and C. Nicolas, "Semi-supervised Method to Detect Fraudulent Transactions and Identify Fraud Types while Minimizing Mounting Costs," International Journal of Advanced Computer Science and Applications, vol. 14, no. 2, Jan. 2023, doi: 10.14569/ijacsa 2023.0140298.
[42] K. S. Deb, S. Ghosal, and D. Bose, "A Comparative Study on Credit Card Fraud Detection," Jun. 2021, doi: 10.31224/osf.io/8ctxd.
[43] P. Joseph, "Artificial Intelligence: The benefits to revenue cycle management," Jan. 2020, Accessed: Dec. 2024. [Online]. Available: https://www.medicaleconomics.com/news/artificial-intelligence-benefits-revenue-cycle-management
[44] B. Kim, S. Sridharan, A. Atwal, and V. Ganapathi, "Deep Claim: Payer Response Prediction from Claims Data with Deep Learning," arXiv (Cornell University), Jan. 2020, doi: 10.48550/arxiv.. 2007.06229.
[45] M. H. Chagahi, N. Delfan, S. M. Dashtaki, B. Moshiri, and Md. J. Piran, "An Innovative Attention-based Ensemble System for Credit Card Fraud Detection," arXiv (Cornell University), Oct. 2024, doi: 10.48550/arxiv.. 2410.09069.
[46] B. Mytnyk, O. Tkachyk, N. Shakhovska, С. Федушко, and Y. Syerov, "Application of Artificial Intelligence for Fraudulent Banking Operations Recognition," Big Data and Cognitive Computing, vol. 7, no. 2, p. 93, May 2023, doi: 10.3390/bdcc7020093.
[47] U. Pagallo et al., "The underuse of AI in the health sector: Opportunity costs, success stories, risks and recommendations," Health and Technology, vol. 14, no. 1, p. 1, Dec. 2023, doi: 10.1007/s12553-023-00806-7.
[48] V.. Kilanko, "The Transformative Potential of Artificial Intelligence in Medical Billing: A Global Perspective," International Journal of Scientific Advances, vol. 4, no. 3, Jan. 2023, doi: 10.51542/ijscia.v4i3.8.
[49] Y.-H. Li, Y. Li, M.-Y. Wei, and G. Li, "Innovation and challenges of artificial intelligence technology in personalized healthcare," Scientific Reports, vol. 14, no. 1. Nature Portfolio, Aug. 16, 2024. doi: 10.1038/s41598-024-70073-7.
[50] A. O. Akinrinmade et al., "Artificial Intelligence in Healthcare: Perception and Reality," Cureus. Cureus, Inc., Sep. 20, 2023. doi: 10.7759/cureus.45594.
[51] S. K. Mudgal, R. Agarwal, J. Chaturvedi, R. Gaur, and N. Ranjan, "Real-world application, challenges, and implications of artificial intelligence in healthcare: an essay." PubMed, vol. 43. National Institutes of Health, p. 3, Jan. 01, 2022. doi: 10.11604/pamj.2022.43.3.33384.
[52] H. Xu, K. Niu, T. Lu, and S. Li, "Leveraging artificial intelligence for enhanced risk management in financial services: Current applications and prospects," Engineering Science & Technology Journal, vol. 5, no. 8, p. 2402, Aug. 2024, doi: 10.51594/estj.v5i8.1363.
[53] W. A. Addy, A. O. Ajayi-Nifise, B. G. Bello, S. T. Tula, O. Odeyemi, and T. Falaiye, "AI in credit scoring: A comprehensive review of models and predictive analytics," Global Journal of Engineering and Technology Advances, vol. 18, no. 2. p. 118, Feb. 20, 2024. doi: 10.30574/gjeta.2024.18.2.0029.
[54] C. F. Mwachikoka, "Effects of artificial intelligence on financial reporting accuracy," World Journal of Advanced Research and Reviews, vol. 23, no. 3, p. 1751, Sep. 2024, doi: 10.30574/wjarr 2024.23.3.2791.
[55] B. O. Adelakun, "THE IMPACT OF AI ON INTERNAL AUDITING: TRANSFORMING PRACTICES AND ENSURING COMPLIANCE," Finance & Accounting Research Journal, vol. 4, no. 6, p. 350, Dec. 2022, doi: 10.51594/farj.v4i6.1316.
[56] L. Lidiana, "AI and Auditing: Enhancing Audit Efficiency and Effectiveness with Artificial Intelligence," Deleted Journal, vol. 1, no. 3, p. 214, Mar. 2024, doi: 10.62207/g0wpn394.
[57] D. Leocádio, L. Malheiro, and J. Reis, "Artificial Intelligence in Auditing: A Conceptual Framework for Auditing Practices," Administrative Sciences, vol. 14, no. 10, p. 238, Sep. 2024, doi: 10.3390/admsci14100238.
[58] N. R. Sahni, G. Stein, R. W. Zemmel, and D. Cutler, "The Potential Impact of Artificial Intelligence on Healthcare Spending," Jan. 2023. doi: 10.3386/w30857.

[59] S. V. Bhagat and D. Kanyal, "Navigating the Future: The Transformative Impact of Artificial Intelligence on Hospital Management- A Comprehensive Review," Cureus. Cureus, Inc., Feb. 20, 2024. doi: 10.7759/cureus.54518.
[60] M. Bekbolatova, J. Mayer, C. W. Ong, and M. Toma, "Transformative Potential of AI in Healthcare: Definitions, Applications, and Navigating the Ethical Landscape and Public Perspectives," Healthcare, vol. 12, no. 2. Multidisciplinary Digital Publishing Institute, p. 125, Jan. 05, 2024. doi: 10.3390/healthcare12020125.
[61] A. Thakkar, A. Gupta, and A. D. Sousa, "Artificial intelligence in positive mental health: a narrative review," Frontiers in Digital Health, vol. 6. Frontiers Media, Mar. 18, 2024. doi: 10.3389/fdgth.2024.1280235.
[62] N. N. Ridzuan, M. Masri, M. Anshari, N. L. Fitriyani, and M. Syafrudin, "AI in the Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility," Information, vol. 15, no. 8, p. 432, Jul. 2024, doi: 10.3390/info15080432.
[63] D. Patil, "Artificial Intelligence In Financial Services: Advancements In Fraud Detection, Risk Management, And Algorithmic Trading Optimization," Jan. 2025, doi: 10.2139/ssrn.5057412.
[64] S. A. Alowais et al., "Revolutionizing healthcare: the role of artificial intelligence in clinical practice," BMC Medical Education, vol. 23, no. 1. BioMed Central, Sep. 22, 2023. doi: 10.1186/s12909-023-04698-z.
[65] S. Kapa, "The Role of Artificial Intelligence in the Medical Field," Journal of Computer and Communications, vol. 11, no. 11, p. 1, Jan. 2023, doi: 10.4236/jcc.2023.1111001.
[66] A. Shuaib, "Transforming Healthcare with AI: Promises, Pitfalls, and Pathways Forward," International Journal of General Medicine, p. 1765, May 2024, doi: 10.2147/ijgm.s449598.
[67] M. Jeyaraman, S. Balaji, N. Jeyaraman, and S. Yadav, "Unraveling the Ethical Enigma: Artificial Intelligence in Healthcare," Cureus. Cureus, Inc., Aug. 10, 2023. doi: 10.7759/cureus.43262.
[68] H. J. Abukhadijah and A. J. Nashwan, "Transforming Hospital Quality Improvement Through Harnessing the Power of Artificial Intelligence," Global Journal on Quality and Safety in Healthcare, vol. 7, no. 3, p. 132, Jun. 2024, doi: 10.36401/jqsh-24-4.
[69] J. Hatherley, "Limits of trust in medical AI," Journal of Medical Ethics, vol. 46, no. 7, p. 478, Mar. 2020, doi: 10.1136/medethics-2019-105935.
[70] E. Hildt, "What Is the Role of Explainability in Medical Artificial Intelligence? A Case-Based Approach," Bioengineering, vol. 12, no. 4, p. 375, Apr. 2025, doi: 10.3390/bioengineering12040375.
[71] C. Giordano, M. Brennan, B. Mohamed, P. Rashidi, F. Modave, and P. J. Tighe, "Accessing Artificial Intelligence for Clinical Decision-Making," Frontiers in Digital Health, vol. 3. Frontiers Media, Jun. 25, 2021. doi: 10.3389/fdgth.2021.645232.
[72] A. Dhopte and H. Bagde, "Smart Smile: Revolutionizing Dentistry With Artificial Intelligence," Cureus. Cureus, Inc., Jun. 30, 2023. doi: 10.7759/cureus.41227.
[73] A. F. Markus, J. A. Kors, and P. R. Rijnbeek, "The role of explainability in creating trustworthy artificial intelligence for health care: A comprehensive survey of the terminology, design choices, and evaluation strategies," Journal of Biomedical Informatics, vol. 113. Elsevier BV, p. 103655, Dec. 10, 2020. doi: 10.1016/j.jbi.2020.103655.
[74] C. Wang et al., "Towards Reliable and Explainable AI Model for Solid Pulmonary Nodule Diagnosis," arXiv (Cornell University), Jan. 2022, doi: 10.48550/arxiv.2204.04219.
[75] H. W. Loh, C. P. Ooi, S. Seoni, P. D. Barua, F. Molinari, and U. R. Acharya, "Application of explainable artificial intelligence for healthcare: A systematic review of the last decade (2011–2022)," Computer Methods and Programs in Biomedicine, vol. 226. Elsevier BV, p. 107161, Sep. 27, 2022. doi: 10.1016/j.cmpb.2022.107161.
[76] M. Liu et al., "Towards clinical AI fairness: A translational perspective," arXiv (Cornell University), Jan. 2023, doi: 10.48550/arxiv.2304.13493.
[77] A. A. Abujaber and A. J. Nashwan, "Ethical framework for artificial intelligence in healthcare research: A path to integrity," World Journal of Methodology, vol. 14, no. 3. Jun. 25, 2024. doi: 10.5662/wjm.v14.i3.94071.
[78] R. I. M. Almoselhy and A. Usmani, "AI in Food Science: Exploring Core Elements, Challenges, and Future Directions," Open Access Journal of Microbiology & Biotechnology, vol. 9, no. 4, p. 1, Oct. 2024, doi: 10.23880/oajmb-16000313.
[79] C. Greenman, D. Esplin, R. Johnston, and J. Richard, "An Analysis of the Impact of Artificial Intelligence on the Accounting Profession," Journal of Accounting Ethics & Public Policy, vol. 25, no. 2, Nov. 2024, doi: 10.60154/jaepp.2024.v25n2p188.
[80] A. E. Artene, A. E. Domil, and L. Ivașcu, "Unlocking Business Value: Integrating AI-Driven Decision-Making in Financial Reporting Systems," Electronics, vol. 13, no. 15, p. 3069, Aug. 2024, doi: 10.3390/electronics13153069.
[81] Z. Wang, "Artificial Intelligence and Machine Learning in Credit Risk Assessment: Enhancing Accuracy and Ensuring Fairness," Open Journal of Social Sciences, vol. 12, no. 11, p. 19, Jan. 2024, doi: 10.4236/jss.2024.1211002.
[82] Y. Han, J. Chen, M. Dou, J. Wang, and K. Feng, "The Impact of Artificial Intelligence on the Financial Services Industry," Deleted Journal, vol. 2, no. 3, p. 83, May 2023, doi: 10.54097/ajmss.v2i3.8741.
[83] N. Polemi, I. Praça, K. Kioskli, and A. Bécue, "Challenges and efforts in managing AI trustworthiness risks: a state of knowledge," Frontiers in Big Data, vol. 7, May 2024, doi: 10.3389/fdata.2024.1381163.
[84] S. M. T. Situmeang, R. Harliyanto, P. D. Zulkarnain, U. Mahdi, and T. Nugroho, "The Role of Artificial Intelligence in Criminal Justice," Global International Journal of Innovative Research, vol. 2, no. 8, p. 1966, Aug. 2024, doi: 10.59613/global.v2i8.264.
[85] D. Petković, "It is Not 'Accuracy vs. Explainability'—We Need Both for Trustworthy AI Systems," IEEE Transactions on Technology and Society, vol. 4, no. 1, p. 46, Jan. 2023, doi: 10.1109/tts.2023.3239921.
[86] Y. Wang, "Ethical considerations of AI in financial decision," Computing and artificial intelligence., vol. 2, no. 1, p. 1290, Jun. 2024, doi: 10.59400/cai.v2i1.1290.
[87] N. Rane, S. Choudhary, and J. Rane, "Artificial Intelligence and Machine Learning in Business Intelligence, Finance, and E-commerce: a Review," SSRN Electronic Journal. RELX Group (Netherlands), Jan. 01, 2024. doi: 10.2139/ssrn.4843988.
[88] M. A. Al-antari, "Artificial Intelligence for Medical Diagnostics—Existing and Future AI Technology!," Diagnostics, vol. 13, no. 4. Multidisciplinary Digital Publishing Institute, p. 688, Feb. 12, 2023. doi: 10.3390/diagnostics13040688.
[89] C. Mennella, U. Maniscalco, G. D. Pietro, and M. Esposito, "Ethical and regulatory challenges of AI technologies in healthcare: A narrative review," Heliyon, vol. 10, no. 4. Elsevier BV, Feb. 01, 2024. doi: 10.1016/j.heliyon.2024.e26297.

[90] D. D. Farhud and S. Zokaei, "Ethical Issues of Artificial Intelligence in Medicine and Healthcare," Iranian Journal of Public Health. Knowledge E, Oct. 27, 2021. doi: 10.18502/ijph.v50i11.7600.
[91] A. A. Kuwaiti et al., "A Review of the Role of Artificial Intelligence in Healthcare," Journal of Personalized Medicine, vol. 13, no. 6. Multidisciplinary Digital Publishing Institute, p. 951, Jun. 05, 2023. doi: 10.3390/jpm13060951.
[92] S. I. Lambert et al., "An integrative review on the acceptance of artificial intelligence among healthcare professionals in hospitals," npj Digital Medicine, vol. 6, no. 1. Nature Portfolio, Jun. 10, 2023. doi: 10.1038/s41746-023-00852-5.
[93] F. Pesapane et al., "Legal and Regulatory Framework for AI Solutions in Healthcare in EU, US, China, and Russia: New Scenarios after a Pandemic," Radiation, vol. 1, no. 4, p. 261, Oct. 2021, doi: 10.3390/radiation1040022.
[94] J. Morley et al., "The ethics of AI in health care: A mapping review," Social Science & Medicine, vol. 260. Elsevier BV, p. 113172, Jul. 15, 2020. doi: 10.1016/j.socscimed.2020.113172.
[95] S. M. Varnosfaderani and M. Forouzanfar, "The Role of AI in Hospitals and Clinics: Transforming Healthcare in the 21st Century," Bioengineering, vol. 11, no. 4, p. 337, Mar. 2024, doi: 10.3390/bioengineering11040337.
[96] C. Elendu et al., "Ethical implications of AI and robotics in healthcare: A review," Medicine, vol. 102, no. 50. Wolters Kluwer, Dec. 15, 2023. doi: 10.1097/md.0000000000036671.
[97] S. Gerke, T. Minssen, and G. Cohen, "Ethical and legal challenges of artificial intelligence-driven healthcare," in Elsevier eBooks, Elsevier BV, 2020, p. 295. doi: 10.1016/b978-0-12-818438-7.00012-5.
[98] C. Régis, "AI and Health Law," SSRN Electronic Journal, Jan. 2021, Accessed: Feb. 2025. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3733964
[99] D. Jha et al., "Ensuring Trustworthy Medical Artificial Intelligence through Ethical and Philosophical Principles," arXiv (Cornell University), Jan. 2023, doi: 10.48550/arxiv.2304.11530.
[100] S. Yelne, M. Chaudhary, K. Dod, A. Sayyad, and R. Sharma, "Harnessing the Power of AI: A Comprehensive Review of Its Impact and Challenges in Nursing Science and Healthcare," Cureus. Cureus, Inc., Nov. 22, 2023. doi: 10.7759/cureus.49252.
[101] L. A. Ossa, G. Lorenzini, S. R. Milford, D. Shaw, B. S. Elger, and M. Rost, "Integrating ethics in AI development: a qualitative study," BMC Medical Ethics, vol. 25, no. 1, Jan. 2024, doi: 10.1186/s12910-023-01000-0.
[102] J. Zhang and Z. Zhang, "Ethics and governance of trustworthy medical artificial intelligence," BMC Medical Informatics and Decision Making, vol. 23, no. 1, Jan. 2023, doi: 10.1186/s12911-023-02103-9.
[103] B. Khan et al., "Drawbacks of Artificial Intelligence and Their Potential Solutions in the Healthcare Sector," Deleted Journal, vol. 1, no. 2. p. 731, Feb. 08, 2023. doi: 10.1007/s44174-023-00063-2.
[104] R. D'Souza, M. Mathew, V. Mishra, and K. M. Surapaneni, "Twelve tips for addressing ethical concerns in the implementation of artificial intelligence in medical education," Medical Education Online, vol. 29, no. 1, Apr. 2024, doi: 10.1080/10872981.2024.2330250.