

Original Article

Using AI to Combat Medicaid Fraud, Waste, and Abuse

Anand Laxman Mhatre

Senior Program Manager / Technical Architect, Accenture, USA.

Received Date: 12 September 2024

Revised Date: 16 October 2024

Accepted Date: 08 November 2024

Abstract: Although traditional fraud detection and prevention methods have been integral in reducing fraud and losses in the Medicaid programs, these methods have weaknesses such as inability to process large quantities of data, the inability to provide real-time monitoring of claims processing, the lack of predictive capabilities, and limitations in leveraging unstructured data. Integration of AI in Medicaid fraud mitigation bridges these limitations. The technology is advanced in data processing, allowing scalability of fraud investigations, real-time monitoring of claims, and forecasting of potential frauds. This publication describes the limitations of traditional Medicaid fraud control methods and how AI can be leveraged to bridge these inefficiencies.

Index Terms: Medicaid, Fraud, AI, Technology, Medicaid Fraud Prevention Methods.

I. INTRODUCTION

Medicaid fraud is an ongoing, decades-old challenge that affects not just CMS but patients as well. For long, unscrupulous healthcare providers have been exploiting strategies such as medical identity theft, billing for unnecessary services or items, billing for services not furnished, upcoding, unbundling, and kickbacks to benefit from Medicaid programs unfairly. According to the National Health Care Anti-Fraud Association, about 3 percent (\$300 billion) of healthcare spending is lost to fraud annually [1]. Although CMS and other stakeholders have attempted to install mechanisms to curb the depravity, evidence suggests that Medicaid programs are still losing billions of dollars. The inefficacy of traditional methods, such as 'pay and chase,' to curb healthcare fraud, waste, and abuse stems from the weaknesses of these methods.

A. Traditional fraud and abuse control methods

Although traditional fraud and abuse control techniques have helped reduce and recover fraud proceeds in Medicaid, these methods fall short in various aspects, allowing healthcare fraud to thrive. Some of the reasons these methods are ineffective include;

a) Inability to process vast amounts of data

Medicaid programs are data intensive. Healthcare providers and payment processing teams generate vast amounts of data that must be audited regularly to detect fraud. Traditional fraud control methods use manual data processing techniques. The ability of human data analysts to process vast amounts of data is limited. The inability to continuously process large quantities of data downgrades payers' capability to reveal suspicious fraud patterns [2].

b) No real-time monitoring

The data processing limitations of manual data processing methods prevent payers from monitoring claims in real time and averting fraud before occurring. Delayed detection of fraud has two impacts. One, once fraud has occurred, recouping payments becomes a complex process. Perpetrators may close operations or even move offshores, making recovery impossible. The cost of recovery may also be astronomical. Audits and legal battles are not only time-consuming but also expensive. Two, the inability to detect and stop fraud in real-time incentivizes fraud. Perpetrators view the risk of being discovered as low compared to the potential reward.

c) Limited fraud prediction capability:

Traditional fraud detection methods are not meant to predict potential schemes. These methods do not have the mechanisms and capabilities to leverage historical data to foresee possible threats. In fact, traditional fraud control methods are designed to be reactive. They can only detect fraud and abuse that has already occurred.

d) Limitations in unstructured data processing

Legacy systems used in fraud detection and control are primarily designed to process structured data. They cannot leverage data sources such as medical notes and images when processing claims. These systems are also not intended to detect inconsistencies in the language used in claims, such as discrepancies between reported conditions and prescribed treatments.



In a nutshell, the physical nature of traditional fraud detection and control methods in healthcare renders them ineffective for combating crime in the sector. Due to limited data processing capabilities, these systems cannot comprehensively analyze all data to unearth fraud, cannot detect anomalies in real-time, and cannot predict potential fraud. The data processing limitations of these methods can be bridged by deploying AI-powered systems in fraud and waste control.

Table 1: Summary of limitations of traditional fraud and waste control methods

Inability to process vast data quantities	Limits ability to scale fraud detection, allowing complex schemes to persist.
No real-time monitoring	Allows fraud to happen. Recouping costs can be high. Incentivizes fraud.
Limited fraud prediction.	Renders fraud detection efforts reactive.
Lack of unstructured data processing	Denies investigators the benefits of unstructured data in detecting fraud.

II. AI IN FRAUD AND WASTE CONTROL

Artificial intelligence is an emerging technology revolutionizing fraud detection and prevention in the financial sector. According to a report by KPMG, AI-powered anti-fraud engines can reduce fraud by as much as 40 percent [3]. Financial institutions employ AI in fraud detection by monitoring patterns and user profiles. Medicaid management can also use AI to detect and prevent Medicaid fraud. The technology can be used to reveal hidden fraud patterns. The technology can also be deployed to track providers' activities, exposing fraud and misuse. Some of the areas AI technologies that can be used to enhance fraud control in Medicaid are;

A. Big data analysis

AI systems can process large data junks to reveal hidden patterns of fraud. The technology allows payers to leverage every nugget of data in fraud detection. AI systems can scan all billing data to reveal unusual patterns or irregularities in provider practices [4]. For example, these systems can detect and raise alerts on providers who frequently bill for high-cost services, schedule unusually high patient volumes, or submit claims for services that are unlikely to occur in such frequency.

B. Predictive analysis

Proper analysis of historical data can reveal patterns that can be used to predict future fraud. AI models can be trained using historical data to predict fraud risks. For example, using insights such as procedures employed by care providers, AI models can rate providers' fraud risk and warn Medicaid administrators on profiles more likely to commit fraud.

C. Real-time monitoring

AI models can process data quickly and provide real-time insights for administrators to act on. They can process claims data as it comes in and detect and block potentially fraudulent activities, safeguarding payers from making payments and later chasing after them. AI's fast data processing has opened the door for real-time claims monitoring.

D. Advanced unstructured data processing

AI models such as Natural Language Processing (NLP) can analyze unstructured text data in claims, medical notes, and patient histories. They can identify potential fraud by analyzing inconsistencies in the language used in claims or discrepancies between prescribed treatments and reported conditions.

E. Data cross-referencing

In some cases, data required to audit the validity of claims is distributed in multiple systems. AI-enabled fraud detection systems often use cross-referenced data from various sources like insurance claims, tax records, and employment data to verify the accuracy of claims. If discrepancies are detected in data held by different systems, related claims are flagged for further investigation. Using external databases, AI systems can also help Medicaid agencies determine patient eligibility.

F. Link Analysis

Some healthcare frauds, such as referrals and kickbacks, involve multiple parties. Detecting relationships between perpetrators using traditional methods can be challenging. AI models can conduct link analysis on providers, patients, and claims, uncovering relationships between seemingly unrelated entities, and identifying fraud rings, where groups of individuals or organizations collude in fraudulent activities.

G. Data visualization and reporting

AI-enabled systems usually have potent data visualization tools. These tools effectively display trends, outliers, and suspicious activity across large volumes of data. Using visualization tools such as graphs, heat maps, and dashboards, investigators and administrators can easily spot anomalies and understand areas to focus their investigations.

Table 2: Summary of how AI aids fraud and waste control

Big data analysis	Scales investigations by allowing use of all available data.
Predictive analysis	Allows proactive mitigation of fraud risks.
Real-time monitoring	Enables real-time prevention of fraud.
Advanced unstructured data processing	Permits use of unstructured data in investigations, expanding the scope of investigations hence improving chances of unearthing fraud.
Data cross-referencing	Expands the scope of investigations.
Link analysis	Map relations between providers to discover fraud syndicates.

III. IMPACT OF AI ON MEDICAID FRAUD CONTROL

Integration of AI in Medicaid fraud detection waste control has a profound impact on the success of fraud control efforts. AI has enhanced the efficiency, accuracy, and scalability of identifying and combating fraudulent activities. Some of the ways the technology is impacting fraud control include;

A. Enhanced Fraud Detection Capabilities:

AI has enhanced Medicaid fraud control by enabling real-time monitoring of claims processing, enabling detection of sophisticated schemes, and reducing the occurrence of false positives, allowing investigators to focus only on legitimate cases.

B. Increased efficiency:

AI has automated data processing, claims review, and initial investigations, freeing human resources for complex tasks. The technology also accelerated data processing, minimizing time wastage on data processing.

C. Scaled investigations:

AI can process vast quantities of data quickly. This allows investigators to accommodate as much data as possible in their investigations.

D. Improved decision-making:

AI enables data-driven decisions. Besides, it minimizes human error and bias in fraud detection processes, promoting objective and consistent decision-making.

E. Cost savings:

It curbs fraud in advance, preventing loss of funds. It also helps investigators to accurately focus on high-risk cases, minimizing chances of investing in unnecessary investigations.

IV. CONCLUSION

Though traditional fraud detection and waste control methods have been integral in reducing fraud and losses in the Medicaid program, these methods have limitations such as inability to process large quantities of data, incapability to provide real-time monitoring of claims processing, lack predictive capabilities, and cannot leverage unstructured data. Integration of AI in Medicaid fraud mitigation bridges these limitations. The technology is advanced in data processing, allowing scalability of fraud investigations, real-time monitoring of claims, and predicting potential fraud. This allows the management to proactively take preventive measures. Although AI can significantly enhance the efficacy of fraud prevention efforts, it is vulnerable to data privacy and bias issues. It is imperative these systems are implemented in accordance to data privacy regulations and are trained using inclusive datasets.

V. REFERENCES

- [1] Kumaraswamy, N., Markey, M. K., Ekin, T., Barner, J. C., & Rascati, K. (2022). Healthcare fraud data mining methods: A look back and look ahead. *Perspectives in health information management*, 19(1).
- [2] Bauder, R., & Khoshgoftaar, T. (2018, July). A survey of medicare data processing and integration for fraud detection. In *2018 IEEE international conference on information reuse and integration (IRI)* (pp. 9-14). IEEE.
- [3] KPMG (2024), Artificial Intelligence Prevents Fraud. Retrieved From: <https://kpmg.com/dk/en/home/insights/2020/04/artificial-intelligence-prevents-fraud-.html>