From detection to prevention

AI that closes gaps and secures Medicare

Harness the power of leading artificial intelligence (AI), real-time analytics, and a user-friendly business interface to help enable investigators and program analysts revolutionize fraud detection and curb improper payments.

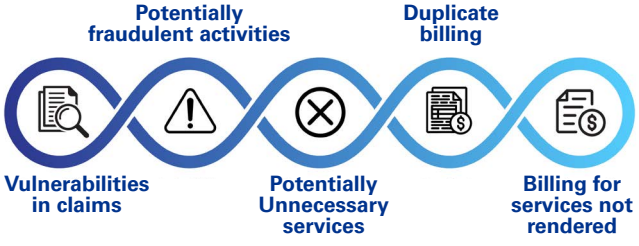
The threat facing Medicare, its beneficiaries, and US taxpayers

Fraud, waste, and abuse (FWA) and improper payments in Medicare cost taxpayers billions annually[1], eroding public trust in federal programs. Increasingly sophisticated fraudsters exploit loopholes via advanced cyber threats and fraud schemes causing potentially catastrophic damage. Addressing FWA, improper payments, and siloed data is critical to restoring integrity and efficiency.

Medicare needs a proactive, scalable, and explainable AI solution that is built on data that has been aggregated, cleansed, and structured to help identify new and evolving fraud patterns and adapt to collusive threats. By enhancing fraud rule indicators and breaking down data silos, the KPMG transparent AI technology application learns with minimal supervision, detects adversarial tactics, and will help enable CMS to stay ahead of evolving fraudsters.

How AI enabled solutions help

Fraud activities are often interconnected and highly sophisticated, which requires continuous monitoring and safeguarding. If applied with a policy-driven, mission-first approach, capabilities enabled by AI can generate investigator-ready rationales, and align findings with agency policies for effective prevention. The KPMG AI-enabled fraud detection technology application identifies:



[1] https://www.gao.gov/fraud-improper-payments

KPMG: A differentiated approach

KPMG offers a forward-looking strategy to modernize oversight, reduce vulnerabilities, and enhance compliance in Medicare. KPMG created a novel AI fraud detection and prevention technology application that combines leading AI research, highly advanced technology, and cybersecurity analytic leads into an all-inclusive application.

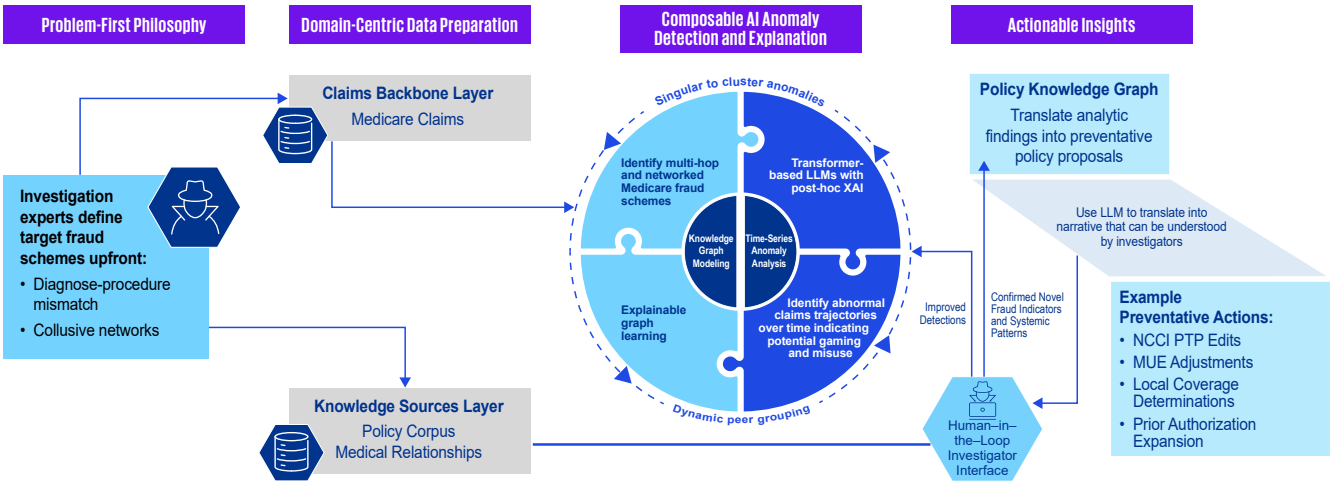
Our innovative AI fraud detection and prevention technology application integrates leading AI research and technology into a unified framework with four components:

1. **Claims Knowledge Graph:**
   Utilizes graph neural networks to detect collusive activities through relational modeling of claims, providers, beneficiaries, and billing codes.
2. **Time-Series Anomaly Detection Engine:**
   Employs transformer-based large language models to identify deviations in claim behavior, signaling potential fraud.
3. **Cybersecurity Analytics Insights Integration:**
   Enriches claims data for better detection of malicious submissions using internet telemetry data.
4. **Policy Knowledge Graph (PKG):**
   Embeds CMS rules into the analytics pipeline to help ensure flagged anomalies are significant and interpretable.

Together, these components form a cohesive application, linking structural anomalies to temporal patterns, and evaluates them against policy constraints for transparent, actionable insights. This enables CMS to advance from detection to proactive prevention with confidence. Together, these components form a closed-loop application where structural anomalies inform temporal baselines; temporal outliers enrich graph features; and both are evaluated against policy constraints to produce transparent, auditable, and actionable insights.

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. USCS036806-3B

The result is a scalable, low-latency, cost-efficient system that can empower AI to unmask and defeat fraud—safeguarding public trust and protecting vital resources.



Ready to make an impact?

Drive meaningful impact in Medicare by modernizing oversight with AI-powered fraud detection—turning fragmented data into actionable insights that protect billions of dollars and restore public trust. The KPMG AI-driven fraud detection engine delivers:

- **Unified data insights** – Bridges siloed data to uncover fraud markers beyond traditional rules-based systems
- **Seamless integration** – Works with existing information technology environments and CMS's cloud-native architecture for cost efficiency
- **Advanced analytics** – Builds a scalable Knowledge Graph and time-series anomaly detection pipeline for real-time oversight
- **Policy alignment** – Leverages the PKG to translate anomaly signals into prepayment actions with clear regulatory rationale
- **Actionable outputs** – Fully explainable insights integrate with program integrity workflows for edit design, provider triage, policy refinement, and vulnerability monitoring.

Let's get started

Healthcare fraud is not only a financial burden but also a threat to public trust and program integrity. By harnessing explainable AI, real-time analytics, and policy-driven insights, federal agencies can move beyond reactive detection to proactive prevention. Our integrated technology application can empower CMS to uncover hidden patterns, adapt to evolving threats, and safeguard billions in taxpayer dollars. The future of healthcare oversight is transparent, scalable, and AI-driven—and it starts now.

Contact KPMG to take the next step

Tom Frame
Principal, Federal Technology Leader
KPMG LLP
T: 610-608-0304
E: tframe@kpmg.com

Sophie Stern
Principal, Federal Healthcare Leader
KPMG LLP
T: 202-809-7425
E: sophiestern@kpmg.com

Ning Wang
Director, Healthcare Data Scientist
KPMG LLP
T: 346-578-3437
E: ningwang1@kpmg.com

Some of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: | **kpmg.com**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2025 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS036806-3B