

WASTE, ABUSE AND FRAUD ARE RAMPANT

Tens of billions of dollars are lost to healthcare fraud, waste, and abuse in the United States each year. The opioid crisis has made the problem worse since fraud is often central to schemes to illegally distribute the medications. A dramatic example came in 2017, Boston Globe uncovered a massive network of brokers who specialized in enrolling multiple patients with phony addresses via healthcare.gov, the Affordable Care Act portal. These patients were signed up for out-of-state insurance plans and enrolled in treatment centers where the administrators provided tens of thousands of dollars in kickbacks per patient to the brokers as well as the physicians who refer the patients. In reality, these patients never receive any care from the treatment center and instead received a kickback for participating in exploiting the insurance companies with generous PPO plans.

Finding these fraudulent activities is challenging. It requires analysis of internal data regarding the patients, opioid treatment facility centers, and referring physicians and connecting it with external data such as recently used addresses and phone numbers to find the hidden connections among patients, doctors, and the opioid treatment facilities.

It also requires benchmarking the end-to-end cost care for every member across a network of doctors and opioid treatment facilities to identify higher than the average cost of care.

DETECTING FRAUD WITH DEEP LINK ANALYSIS

Native parallel graphs, such as TigerGraph, are built to explore and analyze the complex relationships in healthcare data, allowing data scientists and business users to go 10 or more levels deep, across billions of claims and millions of members and prescribers, in real time. The ability to look penetratingly into large data sets by traversing multiple connections in data is called deep link analysis. Consider a doctor who is referring a large portion of patients to a specific substance abuse treatment center specializing in opioid addiction. At first glance there may not appear to be a connection between the substance abuse treatment center and the doctor and traditional fraud solutions can't find anything unusual based on the information available for the doctor, as well as the opioid addiction treatment center.

TigerGraph, however, can mine data from third-party sources such as Thomson Reuters or Dunn and Bradstreet to find all known administrators for the drug treatment center and their current and previous addresses.

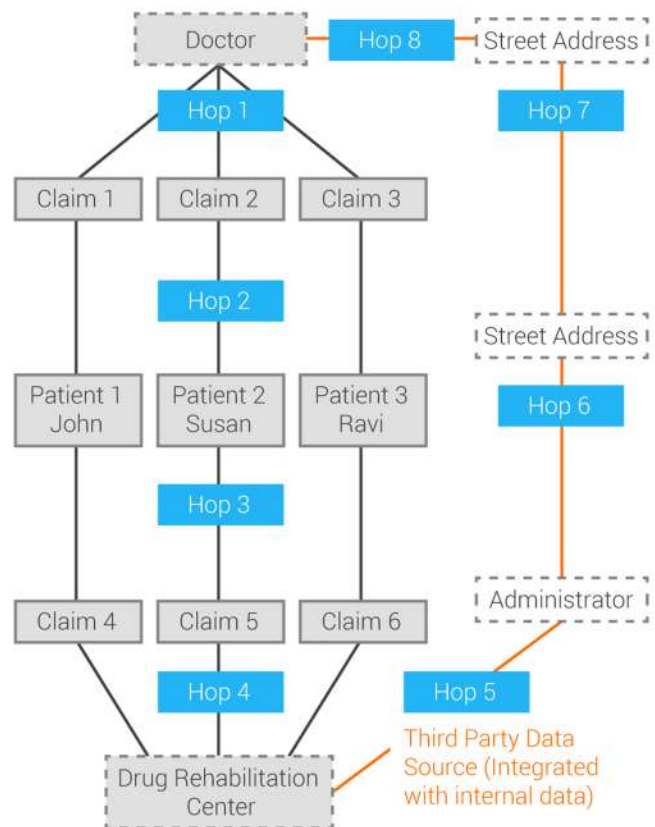


Figure 1: Healthcare organizations can uncover collusion between a prescriber and a treatment facility using deep link analysis

IDENTIFYING FRAUD WITH HUB AND COMMUNITY DETECTION

Another way for a healthcare payer to spot fraud or waste is with hub and community detection - this refers to data connections that are tied to one specific entity. Hub and community detection has two steps: the first step is finding the most influential prescribers (hubs) driving maximum referrals for a specific health condition such as cardiac care or diabetes management or a particular type of drug or healthcare treatment; the second step is establishing a community of connected prescribers and the members availing the services from the prescribers.

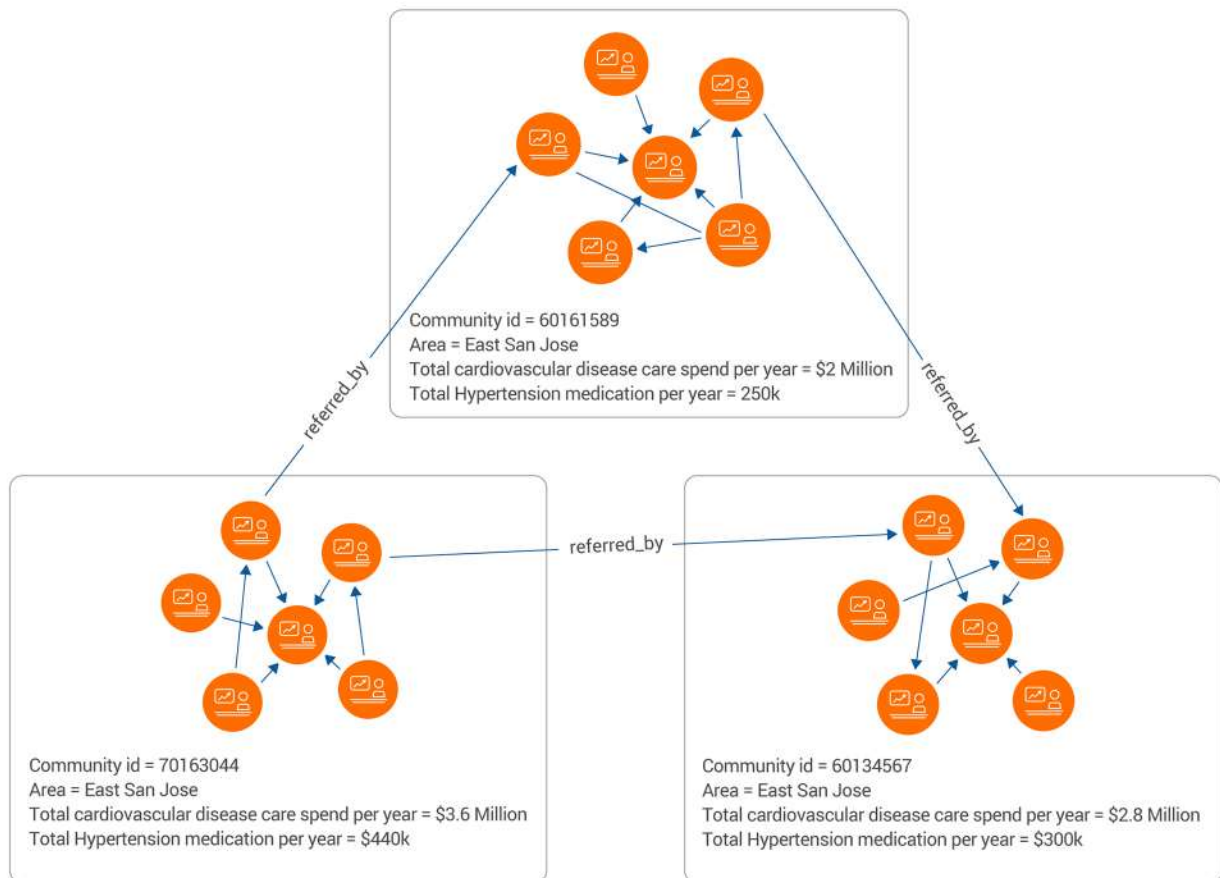


Figure 2: Healthcare organizations can uncover communities of providers and use them to compare the costs of care and identify potential waste and fraud

After that, analysts can establish multiple communities of connected prescribers and understand the healthcare products and services consumed by each community so that they can start to benchmark and compare the average cost of care for a specific health condition such as treatment of type two diabetes or managing hypertension or high blood pressure.

Using TigerGraph, the healthcare payer can start to understand which doctors have above-average spend for the cost of care for similar members, and these insights can be another tool in the toolkit of investigators looking for fraud or waste.

Identifying nefarious practices and taking steps to eliminate them has become a critical priority for healthcare organizations.

APPLYING MACHINE LEARNING TO FRAUD DETECTION

Another tool in the fight against fraud is artificial intelligence. We can generate graph-based machine learning features for a low risk provider (“good doctor”) and a high risk provider (“bad doctor”) and use these features to train the artificial intelligence to look for these profiles within huge healthcare datasets.

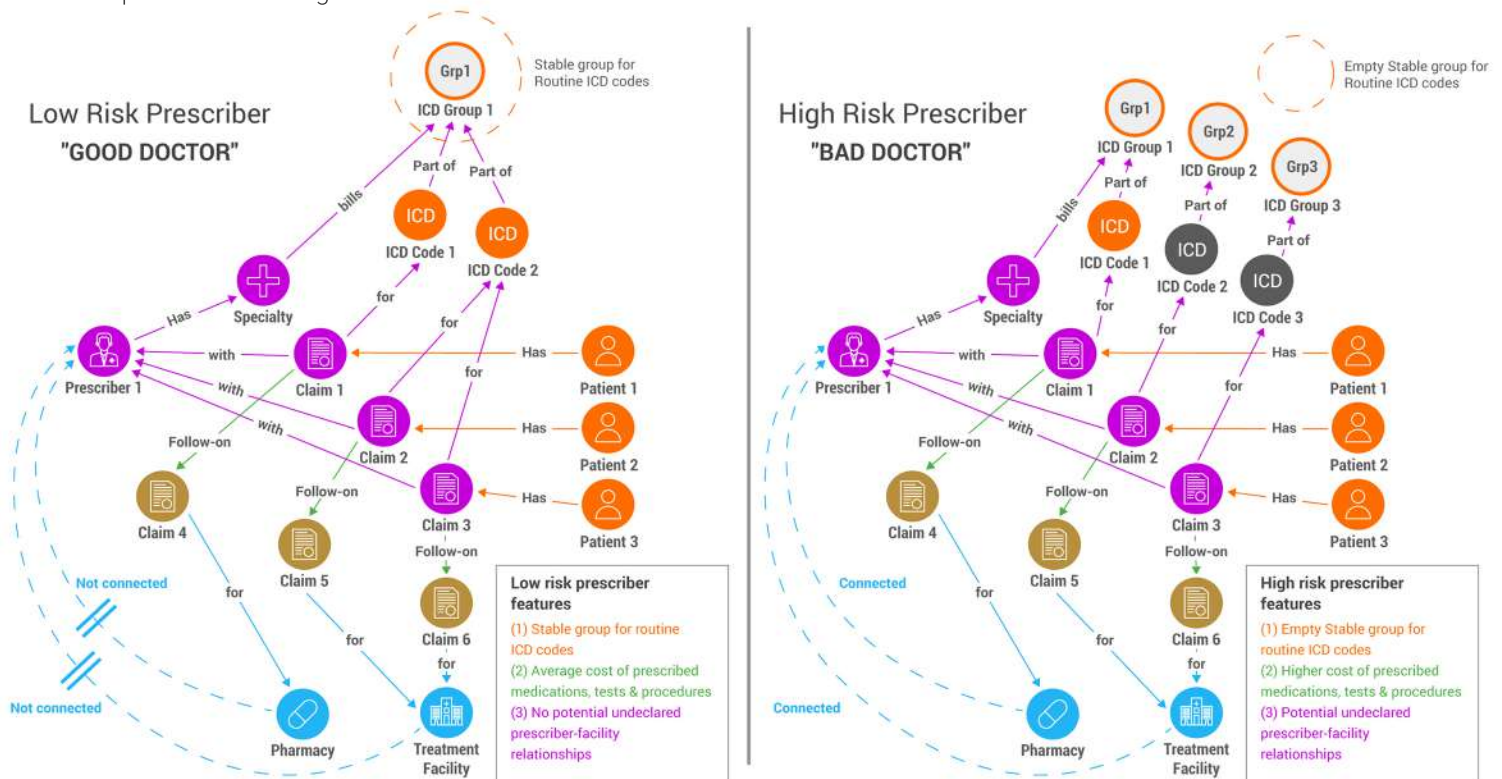


Figure 3: Graph-based analytics can identify low risk providers (“good doctors”) and high risk providers (“bad doctors”)

For example, we can drill down on a feature called “stable group for routine ICD codes.” The stable group includes ICD (International Classification of Diseases) code groups that are billed frequently in claims for the provider over a period of time. The “good doctor” has a stable group with one or more code groups. If a doctor is routinely generating claims for multiple ICD codes that are unrelated to their specialty (such as a podiatrist generating claims for respiratory system and nervous system code groups), they may be a “bad doctor.”

The second feature called “cost of care” compares the cost of prescribed medications, tests and procedures by the prescriber and their referral network with the average cost for treating the healthcare condition for similar members. TigerGraph traverses from the patient to claims, doctors, pharmacies and treatment centers to map out the journey easily, to calculate the cost of care for each provider. Next, the solution finds similar patients and calculates the average cost of care for opioid addiction treatment for each patient population. A “good doctor” has an average cost while a “bad doctor” will have a higher than average cost for the prescribed medications, tests and procedures.

The third feature called “potential undeclared prescriber-facility relationships” digs into undisclosed connections among providers and pharmacies as well as substance abuse facilities. The “good doctor” does not have such connections while a “bad doctor” has undisclosed connections. This was explained earlier as a part of fraud detection with deep link analysis.



The Real-Time Native Parallel Graph

CUSTOMERS



Watch testimonials at tigergraph.com/testimonials

CUSTOMER QUOTES

"It's huge data (*terabytes*) and finding influencers in that data, it's not easy, but TigerGraph has scaled for us."

- Vishnu Maddileti
Director of Data Sciences and Analytics
Amgen

"Some of the questions that graph databases answer are hard to come to conclusion with in RDBMS or it takes forever. We needed a better tool to find relationships and TigerGraph was just that."

- Ely Turkenitz, IS Manager
Santa Clara County

"TigerGraph's speed and scalability and graph model have enabled many applications for us that we previously thought were overly challenging"

- Jack Xie, Head of Data
Wish.com

GET STARTED FOR FREE AT TIGERGRAPH.COM/CLOUD

TigerGraph Cloud graph database as a service is built for agile teams who'd rather be building innovative applications to deliver new insights than managing databases.

CLOUD STARTER KITS

TigerGraph Cloud Starter Kits are built with sample graph data schema, dataset, and queries focused on specific use cases such as fraud detection, recommendation engine, supply chain analysis and/or a specific industry such as healthcare, pharmaceutical or financial services.

Starter Kit	Overview
Customer 360 – Attribution and Engagement Graph	Real-time 360-degree view of the customer journey for attribution and engagement
Cybersecurity Threat Detection-IT	Block cybersecurity threats by detecting interconnected events, devices and people
Enterprise Knowledge Graph (Corporate Data)	Analysis of corporate data including investors and key stakeholders
Enterprise Knowledge Graph (Crunchbase)	Knowledge Graph example featuring Crunchbase data
Entity Resolution (MDM)	Identify, link and merge entities with analysis of attributes and relationships
Financial Services (Payments) – Fraud Detection	Detect and stop fraudulent payments in real-time
Fraud and Money Laundering Detection (Financial Services)	Multiple types of fraud and money laundering patterns
GSQ 101	Introduction to TigerGraph's powerful graph query language
Healthcare Graph (Drug Interaction /FAERS)	Focused on public (FAERS) and private data for pharmaceutical drugs
Healthcare – Referral Networks, Hub (PageRank) & Community Detection	Analyze patient claims to establish referral networks, identify influential doctors
Machine Learning and Real-time Fraud Detection	Mobile industry example for detecting fraud in real-time and for machine learning
Network and IT Resource Optimization	Network and IT resource graph for analyzing the impact of hardware outages
Recommendation Engine (Movie Recommendation)	Graph-based movie recommendation engine built with public data
Social Network Analysis	Social network example for understanding and analyzing relationships
Supply Chain Analysis	Example covering inventory planning and impact analysis

About TigerGraph

TigerGraph is the only scalable graph database for the enterprise. Based on the industry's first Native and Parallel Graph technology, TigerGraph unleashes the power of interconnected data, offering organizations deeper insights and better outcomes. TigerGraph fulfills the true promise and benefits of the graph platform by tackling the toughest data challenges in real-time, no matter how large or complex the dataset. TigerGraph's proven technology supports applications such as fraud detection, customer 360, MDM, IoT, AI and machine learning to make sense of ever-changing big data, and is used by customers including Amgen, China Mobile, Intuit, and Wish, along with some of the world's largest healthcare, entertainment and financial institutions.

CONTACT

TigerGraph
3 Twin Dolphin Drive, Suite 225
Redwood City, California 94065
United States

www.tigergraph.com