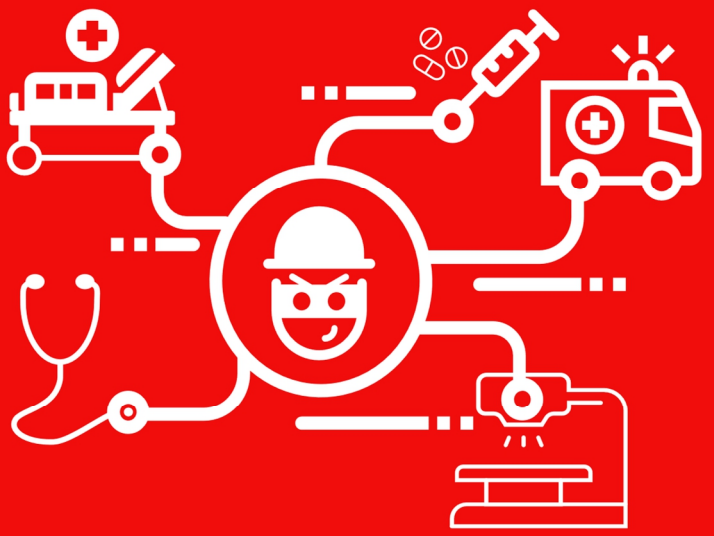


UNIVERSITY OF TWENTE.

Data-Driven Models, Techniques, and Design Principles for Combatting Healthcare Fraud

Thornton

DATA-DRIVEN MODELS, TECHNIQUES, AND DESIGN PRINCIPLES FOR COMBATTING HEALTHCARE FRAUD

Dallas Deverieux Thornton

DATA-DRIVEN MODELS, TECHNIQUES, AND DESIGN PRINCIPLES FOR COMBATTING HEALTHCARE FRAUD

Dallas Deverieux Thornton

DATA-DRIVEN MODELS, TECHNIQUES, AND DESIGN PRINCIPLES FOR COMBATTING HEALTHCARE FRAUD

DISSERTATION

to obtain
the degree of doctor at the University of Twente,
on the authority of the rector magnificus,
prof. dr. ir. A. Veldkamp,
on account of the decision of the Doctorate Board
to be publicly defended
on Friday 8 March 2024 at 16.45 hours

by

Dallas Deverieux Thornton

This dissertation has been approved by:

Promotor
prof. dr. J. van Hillegersberg

Co-promotor
prof. dr. R. M. Müller

Cover design: Dallas Deverieux Thornton
Printed by: Ipskamp Printing
Lay-out: Dallas Deverieux Thornton
ISBN (print): 978-90-365-6015-3
ISBN (digital): 978-90-365-6016-0
URL: https://doi.org/10.3990/1.9789036560160

Graduation Committee

Chair / Secretary:

prof. dr. T. Bondarouk

Promotor:

prof. dr. J. van Hillegersberg
Universiteit Twente, BMS, Industrial Engineering & Business Information Systems

Co-promotor:

prof. dr. R. M. Müller
Berlin School of Economics and Law, Information Systems

Committee Members:

prof. dr. ir. B. P. Veldkamp
Universiteit Twente, BMS, Cognition, Data and Education

prof. dr. ir. E. W. Hans
Universiteit Twente, BMS, Industrial Engineering & Business Information Systems

prof. dr. M. Junger
Universiteit Twente, BMS, Industrial Engineering & Business Information Systems

prof. dr. B. Dinter
University of Technology, Chemnitz, Business Information Systems

dr. C. Amrit
University of Amsterdam, Economics and Business, Business Analytics

Summary

In the U.S., approximately $700 billion of the $2.7 trillion spent on healthcare is linked to fraud, waste, and abuse (Kelley, 2009). This presents a significant challenge for healthcare payers, including governments, insurers, and businesses, as they navigate fraudulent activities from dishonest practitioners, sophisticated criminal networks, and even well-intentioned providers who inadvertently submit incorrect billing for legitimate services. Government-run programs are particularly vulnerable to fraud, given the challenges in excluding problematic providers compared to private networks.

The system's complexity, diversity of actors, and sparsity of labeled data make applying data analysis methods used in other sectors challenging. However, with careful engineering and ongoing adjustments, data analysis techniques such as outlier detection can support programs in controlling escalating costs and maintaining financial stability. This thesis adopts Hevner's (2004) research methodology to guide the creation, assessment, and refinement of a healthcare fraud detection framework and recommended design principles for fraud detection in other similarly complex environments. The thesis provides the following significant contributions to the field:

1. A formal literature review of the field of fraud detection in Medicaid. Chapters 3 and 4 provide formal reviews of the available literature on healthcare fraud. Chapter 3 focuses on defining the types of fraud found in healthcare. Chapter 4 reviews fraud detection techniques in literature across healthcare and other industries. Chapter 5 focuses on literature covering fraud detection methodologies utilized explicitly in healthcare.

2. A multidimensional data model and analysis techniques for fraud detection in healthcare. Chapter 5 applies Hevner et al. (2004) to help develop a framework for fraud detection in Medicaid that provides specific data models and techniques that identify the most prevalent fraud schemes. Based on the environment and knowledge base analysis, a multidimensional schema based on Medicaid data and a set of multidimensional models and techniques to detect fraud in large sets of claim transactions are presented. These artifacts are evaluated through

functional testing against known fraud schemes. This chapter contributes a set of multidimensional data models and analysis techniques that can be used to detect the most prevalent known fraud types.

3. A framework for deploying outlier-based fraud detection methods in healthcare. Chapter 6 proposes and evaluates methods for applying outlier detection to healthcare fraud based on literature review, comparative research, direct application on healthcare claims data, and known fraudulent cases. Based on a multi-dimensional data model developed for Medicaid claim data (Thornton et al., 2013), a method for outlier-based fraud detection is presented and evaluated using Medicaid dental claims, providers, and patients in an actual US state Medicaid program.

4. Design principles for fraud detection in complex systems. Based on literature and applied research in Medicaid healthcare fraud detection, Chapter 7 offers generalized design principles for fraud detection in similar complex, multi-stakeholder systems.

Samenvatting

In de VS wordt van de $2,7 biljoen die aan gezondheidszorg wordt uitgegeven, ongeveer $700 miljard in verband gebracht met fraude, verspilling en misbruik (Kelley, 2009). Dit vormt een aanzienlijke uitdaging voor zorgverzekeraars, waaronder overheden, verzekeraars en bedrijven, terwijl ze frauduleuze activiteiten van oneerlijke praktijkvoerders, gesofisticeerde criminele netwerken en zelfs goedbedoelende aanbieders die per ongeluk onjuiste facturering indienen voor legitieme diensten, navigeren. Overheidsprogramma's zijn bijzonder kwetsbaar voor fraude, gezien de uitdagingen bij het uitsluiten van problematische aanbieders in vergelijking met private netwerken.

De complexiteit van het systeem, de diversiteit van actoren en de schaarste aan gelabelde gegevens maken het toepassen van datananalysemethoden die in andere sectoren worden gebruikt uitdagend. Echter, met zorgvuldige engineering en voortdurende aanpassingen, kunnen datanalysetechnieken zoals afwijkingsdetectie programma's ondersteunen bij het beheersen van escalerende kosten en het handhaven van financiële stabiliteit. Deze thesis neemt Hevner's (2004) onderzoeksmethodologie aan om de creatie, beoordeling en verfijning van een kader voor fraudeopsporing in de gezondheidszorg te begeleiden en aanbevolen ontwerpprincipes voor fraudeopsporing in andere soortgelijk complexe omgevingen. De thesis biedt de volgende significante bijdragen aan het veld:

1. Een formele literatuurstudie van het veld van fraudeopsporing in Medicaid. Hoofdstukken 3 en 4 bieden formele reviews van de beschikbare literatuur over gezondheidszorgfraude. Hoofdstuk 3 focust op het definiëren van de soorten fraude die in de gezondheidszorg worden gevonden. Hoofdstuk 4 beoordeelt fraudeopsporingstechnieken in literatuur over gezondheidszorg en andere industrieën. Hoofdstuk 5 focust op literatuur die specifiek fraudeopsporingsmethodologieën in de gezondheidszorg behandelt.

2. Een multidimensionaal datamodel en analysetechnieken voor fraudeopsporing in de gezondheidszorg. Hoofdstuk 5 past Hevner et al. (2004) toe om een kader voor fraudeopsporing in Medicaid te ontwikkelen dat specifieke datamodellen en technieken biedt die de meest

voorkomende fraudeplannen identificeren. Gebaseerd op de analyse van de omgeving en kennisbasis, wordt een multidimensionaal schema gebaseerd op Medicaid-gegevens en een set van multidimensionale modellen en technieken om fraude in grote sets van claimtransacties te detecteren gepresenteerd. Deze artefacten worden geëvalueerd door middel van functionele tests tegen bekende fraudeplannen. Dit hoofdstuk draagt een set van multidimensionale datamodellen en analysetechnieken bij die kunnen worden gebruikt om de meest voorkomende bekende fraude types te detecteren.

3. Een kader voor het implementeren van op afwijkingen gebaseerde fraudeopsporingsmethoden in de gezondheidszorg. Hoofdstuk 6 stelt methoden voor en evalueert deze voor het toepassen van afwijkingsdetectie op gezondheidszorgfraude, gebaseerd op literatuurstudie, vergelijkend onderzoek, directe toepassing op gegevens van gezondheidszorgclaims en bekende frauduleuze gevallen. Gebaseerd op een multidimensionaal datamodel ontwikkeld voor Medicaid claimgegevens (Thornton et al., 2013), wordt een methode voor op afwijkingen gebaseerde fraudeopsporing gepresenteerd en geëvalueerd met gebruik van Medicaid tandheelkundige claims, aanbieders en patiënten in een daadwerkelijk Amerikaans staats Medicaid-programma.

4. Ontwerpprincipes voor fraudeopsporing in complexe systemen. Gebaseerd op literatuur en toegepast onderzoek in Medicaid gezondheidszorgfraudeopsporing, biedt hoofdstuk 7 gegeneraliseerde ontwerpprincipes voor fraudeopsporing in vergelijkbare complexe, multi-stakeholdersystemen.

Acknowledgments

I want to thank everyone who has supported and contributed to this comprehensive work.

Firstly, I must express my heartfelt thanks to my promoters, prof. dr. Jos van Hillegersberg and prof. dr. Roland Mueller. Your unwavering support throughout the lengthy duration of this project has been invaluable. Jos, your innovative spirit and ability to forge new connections have generated numerous opportunities and relationships. Witnessing your entrepreneurial journey into unknown territories has been truly inspiring! Roland, your directness, humor, and systematic approach to problem-solving have been greatly appreciated. I am grateful for the insights and hospitality you and Katja have provided over the years, and I look forward to maintaining our friendship.

I also wish to thank my thesis committee, prof. dr. Bernard Veldkamp, prof. dr. ir. Erwin Hans, prof. em. dr. Marianne Junger, prof. dr. Barbara Dinter, and dr. Chintan Amrit. Your guidance and expertise have been crucial, whether in the early or final phases of this decade-long journey. Your input has ensured that my work is communicated with precision and rigor.

Special thanks to the innovative thinkers in federal and state agencies committed to enacting positive change. Despite facing significant challenges, your courage and determination have not gone unnoticed. To Jim Gorman, Chris Bunnell, Yohannes Birre, Ashley Corbin, Henry Chao, Mike Mellor, Melissa Fannin, Robin Raveendran, and numerous other government partners, both past and present, your efforts are truly commendable and vital.

My former San Diego Supercomputer Center colleagues at the University of California, San Diego, also deserve a special mention. Jim Daoust, Sandeep Chandra, Natasha Balac, Winston Armstrong, Chris Bunnel, Crystal Brann, Jit Bhattacharya, Steve Lanning, Doug Weimer, Andrew Ferbert, Stephanie Sides, Julie Van Fleet, and many others contributed to this effort. Your dedication to our shared projects has been instrumental in the success of this work. I am grateful for the years we spent working together.

I want to acknowledge the University of Twente's master's students who contributed to the anti-fraud program and are cited in this thesis. Peter Travaille started it off, blazing the path for a Dutch revolution of the project team in San Diego. Paulus Schoutsen brought his big personality and wit to the beach next. The ever-serious Guido van Capelleveen was the last of the Dutch transplants to join us in San Diego for his master's work. Michel Brinkhuis joined me in South Carolina to see first-hand the challenges of making progress in Medicaid at a state level. Your commitment to our shared cause has been invaluable. I cherish our time together and look forward to reconnecting soon.

Thanks to my mom, Debbie, who has dedicated her life to education and always encouraged learning. Thanks to my dad, Larry, for his kindness and constant support. He is watching now from above after enjoying a great visit to Enschede with me early on in this journey.

To my incredible wife, Stacey, your patience and support during the countless trips, long weekends, and late nights have been my pillar of strength. I am eternally grateful.

Lastly, I want to thank my five new family members, Arielle, Noelle, Dallas Jr., Isabelle, and Annabelle. Your sacrifices in support of this thesis have not gone unnoticed. I hope introducing Dutch treats like poffertjes and stroopwafels has sparked your curiosity to explore and embrace diverse cultures and experiences. You are all remarkable, and I look forward to supporting you in your future endeavors, just as you have helped me in mine.

Contents

1

Chapter 1: Introduction

Chapter 1: Introduction

1.1 Background

My fascination with healthcare began years ago, fueled by my discontent with the complexity and costliness of the US healthcare system. I was inspired by the potential to enhance the quality and accessibility of care. The third-party payer system, encompassed by many entities responsible for providing and financing care, has unfortunately cultivated a system more attuned to bill payments than optimizing patient experiences. With trillions of dollars circulating annually, this system is highly susceptible to fraud, waste, and abuse.

Compared to other nations with an average healthcare expenditure of 9.5% of their Gross Domestic Product (GDP), the US stands at 17.6% (Organisation for Economic Co-operation and Development, 2012). Medicare and Medicaid, governmental health insurance programs for the elderly and low-income individuals, supported over 72 million people and accounted for about one-third of the national healthcare spending in 2012 (Truffer et al., 2013). Such large-scale programs inevitably become targets for fraudulent activities. Recognizing this, the Government Accountability Office (GAO) labeled Medicare and Medicaid as high-risk programs due to their size and systemic complexity (U.S. Government Accountability Office, 2012). Astonishingly, nearly a third of all US healthcare expenditures are lost to fraud, waste, and abuse (Kelley, 2009).

Fraud control is a risk management activity akin to others but has unique challenges. In June 2002, Donald Rumsfeld, then United States Secretary of Defense, succinctly addressed the challenge (Rumsfeld, 2002): “The message is that there are no ‘knowns’. There are things we know that we know. There are known unknowns. That is to say, there are things that we now know we don't know. But there are also unknown unknowns. There are things we don't know we don't know. So when we do the best we can, and we pull all this information together, and we then say, well, that's basically what we see as the situation, that is really only the known knowns and the known unknowns. And each year, we discover a few more of those unknown unknowns.”

Healthcare administrators combating fraud face this dilemma of “unknown unknowns.” It necessitates the innovative integration, mastering, and utilizing new and existing data to unveil these hidden challenges. Although the battle between fraud control and perpetrator evasion tactics is ongoing, we can make significant strides in identifying potential fraudulent patterns, eliminating system vulnerabilities, and targeting known bad actors.

Fraud manifests in various forms, including dishonest healthcare providers, unethical administrative practices, and organized criminals. Medicaid, run by states and partially funded by the federal government, is particularly vulnerable due to its patient demographic and less stringent payer oversight than commercial insurers. Even a modest reduction in this pervasive issue can yield significant societal benefits, taxpayer relief, and enhanced patient experience, ultimately allowing genuine healthcare providers to concentrate more on patient care than administrative tasks.

I had the opportunity to work in-depth with Medicaid programs on fraud control methods and systems from 2007 to 2014, developing national systems and processes to assist states and the federal government in the fight against fraud, waste, and abuse. I began this research searching for systematic methods to detect and, optimally, prevent fraudulent activity in healthcare. This thesis describes some techniques developed and lessons learned in the practical fight against healthcare fraud. It also offers approaches outside of fraud control that employers could take to control costs and improve care delivery.

From 2007 to 2014, I worked extensively with Medicaid programs, devising methods and systems to combat fraud, waste, and abuse at both state and federal levels. This journey began with a quest for systematic strategies to detect and ideally prevent fraudulent activities in healthcare. This thesis delves into the developed methodologies and acquired insights from this practical battle against healthcare fraud.

1.2 Research Overview

The U.S. Department of Health and Human Services defines fraud as “the intentional deception or misrepresentation made by an individual who knows it to be false or does not believe it to be true, and makes the false

statement knowing it could result in an unauthorized benefit to oneself or another person" (Department of Health and Human Services, 1998).

Healthcare insurance fraud is a significant issue, resulting in inflated and continuously rising costs for medical insurance programs. Reviewing individual claims or providers is challenging, with an estimated 5 billion claims processed daily. This necessitates the implementation of automated pre-payment controls and enhanced post-payment decision-support tools to facilitate expert analysis.

Despite the prevalence of fraud in the system, state and federal governments lack advanced fraud control systems. Current systems are relatively static, do not offer real-time detection, and focus narrowly on specific claim transactions, neglecting to analyze patterns of suspicious behavior over time or examine the interactions between relevant entities.

Current standard detection and control systems are inadequate for addressing various types of criminal fraud (Hyman, 2001). Automated claims processing systems, equipped with electronic "edits" and "audits," are designed with honest providers in mind. Their purpose is to catch errors and promptly reimburse legitimate providers—ensuring eligibility, verifying that procedure codes match diagnoses, and checking that charges are within acceptable limits—not to uncover patterns indicative of fraudulent or abusive behavior (Sparrow, 2000). This flaw allows individuals with fraudulent intentions to submit claims that appear legitimate, thus evading detection (Sparrow, 2000).

Combating healthcare fraud requires addressing fraudulent practitioners, organized criminal schemes, and well-intentioned providers who make accidental errors. The complexity of physician participation in government programs makes removing problematic providers more difficult than privately managed networks. Despite significant investment in the Health Care Fraud and Abuse Control (HCFAC) program, the impact of these efforts is arguably limited (Sparrow, 2000).

Data analysis methods deployed in other sectors have yet to be widely utilized in this domain. This has been blamed, in part, on the high level of subject matter expertise needed to adapt these techniques to the healthcare field and the peculiarities of a third-party payer system.

However, with up-front engineering and ongoing adaptations, techniques such as outlier detection are suggested as effective predictors for fraud and offer a lifeline to programs struggling to rein in spiraling costs and remain solvent (Bolton & Hand, 2002; Li et al., 2008; Travaille et al., 2011).

While there is extensive literature on data mining and outlier detection techniques (Aggarwal, 2013; Chandola et al., 2009), there needs to be more research on the systematic application and evaluation of these techniques in healthcare. This thesis introduces a data model and methods for applying outlier detection to healthcare fraud, drawing from comparative research, real fraud cases, and literature review for evaluation.

1.3 Approach and Outline of the Thesis

The research methodology proposed by Hevner et al. (2004) was selected to guide the design and enhancement of a fraud detection construct. This construct is refined based on feedback from the environment and continuously updated knowledge. The thesis structure, mapped within Hevner's Design Science Research framework, is illustrated in Figure 1.

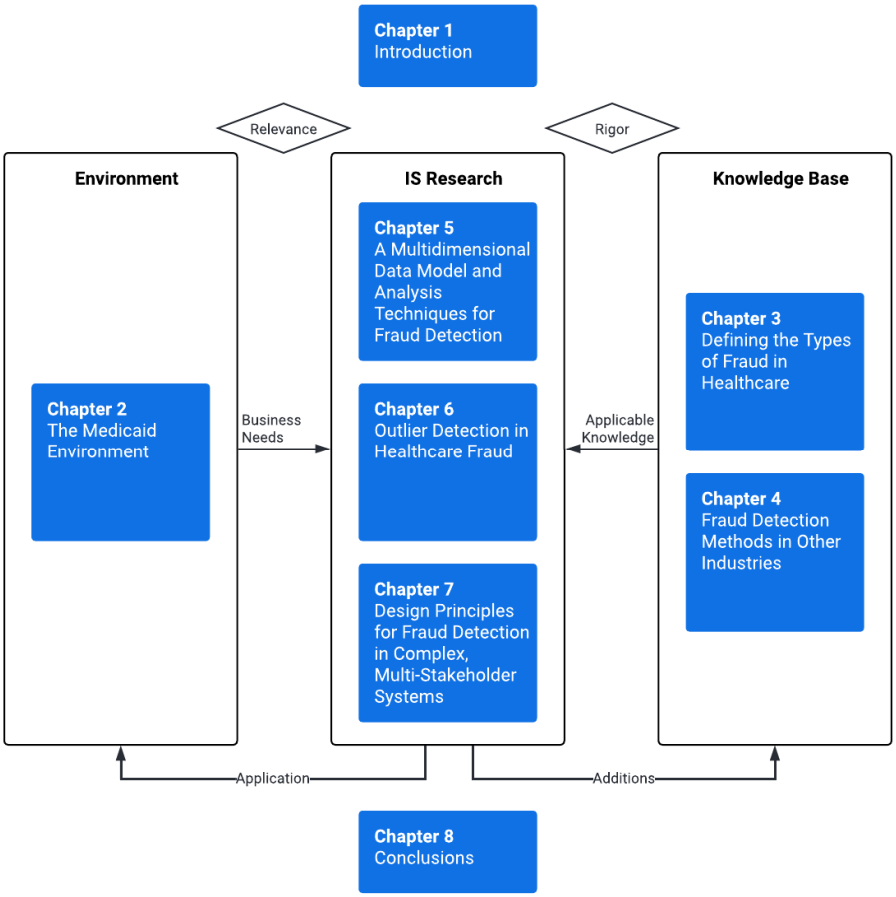


Figure 1 - Thesis Map

The thesis consists of the following chapters:

Chapter 2 provides an insight into the U.S. Medicaid healthcare system. This chapter elaborates on critical actors in the system, their inter-relationships, the processes involved in acquiring care, reimbursement requests, claims payments, and fraud control mechanisms. It also delves into current technologies deployed for claims processing and fraud control.

Chapter 3 offers a comprehensive literature review of the various types of fraud prevalent in healthcare. Utilizing the structured review method Webster and Watson (2002) outlined, a concept matrix was designed to identify different health insurance fraud schemes. The focus was on

literature discussing various forms of health insurance fraud, especially those related to healthcare, health insurance, or the Medicaid program.

Chapter 4 presents a literature review on fraud detection methods in healthcare and other industries. The review employs top-down (keyword-based) and bottom-up (citation analysis) search approaches. It encompasses diverse sectors like finance, telecommunications, healthcare, and computer intrusion detection. Exclusion criteria included articles older than 15 years and papers focusing on algorithmic data mining without an emphasis on or application to fraud detection.

Chapter 5 applies Hevner's (Hevner et al., 2004) Design Science Research framework to guide the development of a multidimensional data model and analysis techniques for healthcare fraud detection. The proposed artifacts are evaluated functionally through testing against known fraud patterns.

Chapter 6 employs the design science research methodology (DSRM) process (Peffers et al., 2007) to Medicaid provider fraud detection. The unique challenges of Medicaid fraud detection are highlighted, emphasizing the need for structured detection methods. A method for applying outlier detection to healthcare fraud is presented, along with a prototype that illustrates the technique. A case study then applies the process to all Medicaid dental providers in a state to evaluate efficacy. The results of the case study are explored, demonstrating the successful identification of fraudulent activity.

Chapter 7 conceptualizes and puts forth design principles for fraud detection in complex systems, generalizing my learnings from work in Medicaid and relevant literature.

Chapter 8 concludes the thesis, evaluates its contributions to design science, and suggests possible avenues for future research.

1.4 Contributions

This thesis provides the following significant contributions:

1. A formal literature review of the field of fraud detection in Medicaid.

Chapters 3 and 4 provide formal reviews of the available literature on healthcare fraud. Chapter 3 focuses on defining the types of fraud found in healthcare. Chapter 4 reviews fraud detection techniques in literature across healthcare and other industries. Chapter 5 focuses on literature covering fraud detection methodologies utilized explicitly in healthcare.

2. A multidimensional data model and analysis techniques for fraud detection in healthcare.

Chapter 5 applies Hevner et al. (Hevner et al., 2004) to help develop a framework for fraud detection in Medicaid that provides specific data models and techniques that identify the most prevalent fraud schemes. Based on the environment and knowledge base analysis, a multidimensional schema based on Medicaid data and a set of multidimensional models and techniques to detect fraud in large sets of claim transactions are presented. These artifacts are evaluated through functional testing against known fraud schemes. This chapter contributes a set of multidimensional data models and analysis techniques that can be used to detect the most prevalent known fraud types.

3. A framework for deploying outlier-based fraud detection methods in healthcare

Chapter 6 proposes and evaluates methods for applying outlier detection to healthcare fraud based on literature review, comparative research, direct application on healthcare claims data, and known fraudulent cases. Based on a multi-dimensional data model developed for Medicaid claim data (Thornton et al., 2013), a method for outlier-based fraud detection is

presented and evaluated using Medicaid dental claims, providers, and patients in an actual US state Medicaid program.

4. Design principles for fraud detection in complex systems

Based on literature and applied research in Medicaid healthcare fraud detection, Chapter 7 offers generalized design principles for fraud detection in similar complex, multi-stakeholder systems.

2

Chapter 2: The Medicaid Environment

Chapter 2: The Medicaid Environment

2.1 Introduction

Winston Churchill once said, referring to Russia then, “It is a riddle, wrapped in a mystery, inside an enigma; but perhaps there is a key. That key is Russian national interest.” (Churchill, 1939) In truth, the US healthcare system is not so different. It is a system comprising many different actors playing different roles with other incentive systems in place, each acting in self-interest. This chapter discusses the environment in which Medicaid exists: the people and organizations involved, along with the roles, incentives, characteristics, structures, culture, processes, and technologies that frame decision-making. State Medicaid “Program Integrity” (fraud control units) are explored, and some systemic disincentives to fraud control improvements are discussed.

2.2 Medicaid History and the Affordable Care Act

The US healthcare system comprises many entities, each with its agenda and looking out for its self-interest. While the system is lauded as one of the best in the world in terms of care, it is unsurprising that its cost of care is one of the highest.

Figure 2 is an infographic published in The New Republic that portrays US healthcare system entities and inter-relationships.

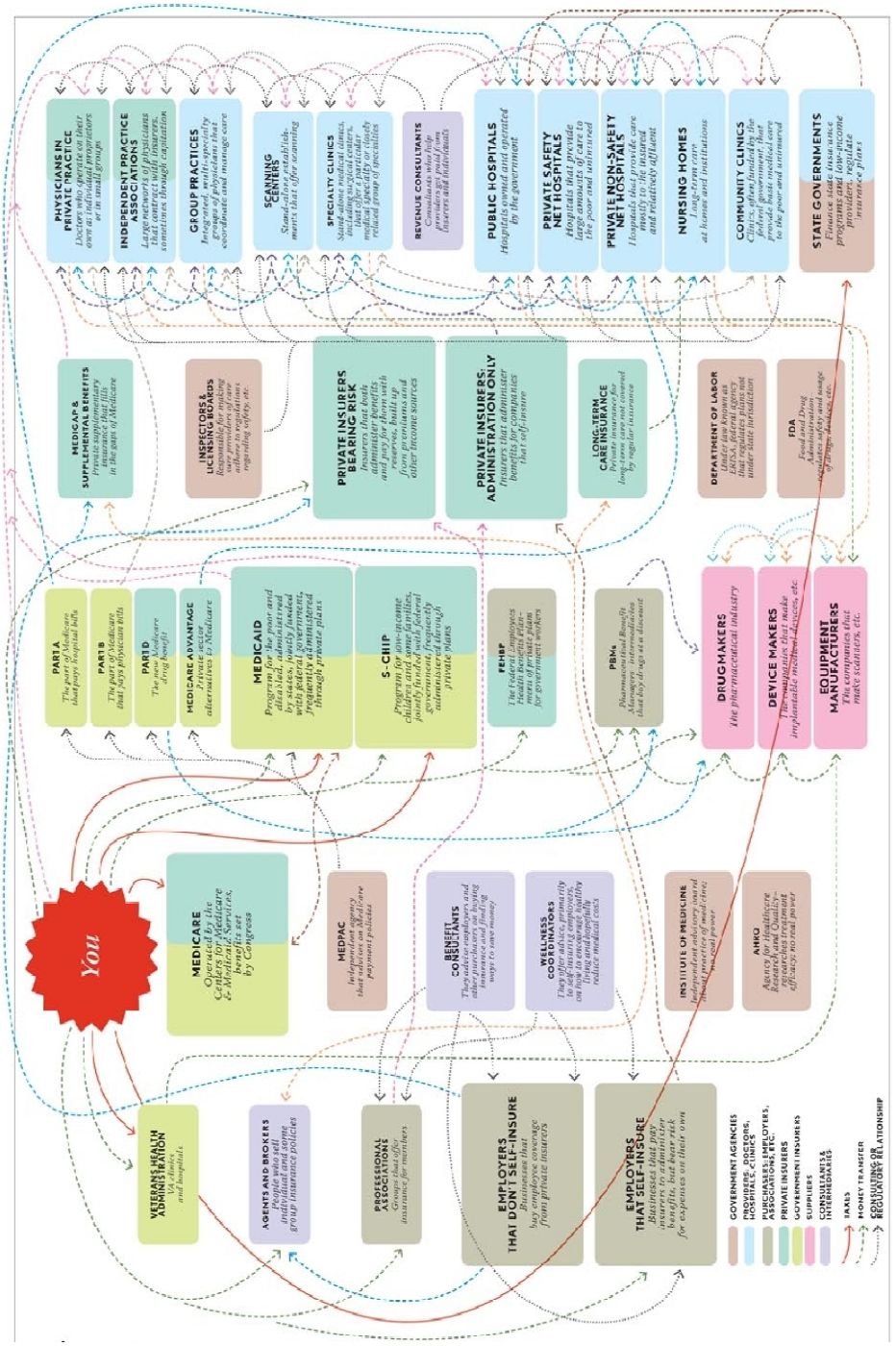


Figure 2 - Your Health Care System: A Map (Cohn, 2009)

2.2.1 History of Medicaid

Established in 1965 by Title XIX of the Social Security Act, Medicaid aims to provide medical assistance to specific low-income individuals and families, including children, pregnant women, and the aged, blind, or disabled. It operates as a healthcare plan administered separately by each state, with significant funding from federal matching funds. Although states are not mandated to participate in Medicaid, all 50 states do so.

Each state sets its eligibility criteria and coordinates program characteristics with the federal Centers for Medicare and Medicaid Services. Individuals receiving Adult Public Assistance or Supplemental Security Income automatically qualify for Medicaid. In contrast, others may gain access through means-testing, often based on their income relative to the federal poverty level.

In 1990, the Omnibus Budget Reconciliation Act established the Health Insurance Premium Payment Program (HIPP) and the Medicaid Drug Rebate Program to reduce Medicaid's expenditures on outpatient drugs. This act added Section 1927 to the Social Security Act of 1935, effective January 1, 1991. Further amendments were made in 1993, mandating states to implement Medicaid estate recovery programs to reclaim medical care costs paid by Medicaid from the estates of deceased beneficiaries. (Thompson/MEDSTAT, 2005)

U.S. Supreme Court decisions and subsequent federal provisions have also mandated Medicaid programs to reimburse schools for services provided to Medicaid-eligible disabled and special-education children.

In the early/mid-90s, President Clinton championed further nationalized healthcare reform, including Medicaid changes. He gave a State of the Union address on January 25, 1994, extolling the virtues of his healthcare plan. He had not planned on Senate Majority Leader Bob Dole's State of the Union Response (Dole, 1994). In it, Dole provided a visual depiction of the already-complicated healthcare system that looks much like Figure 2. This presentation and the subsequent national dialogue essentially closed the door on President Clinton's attempt to control US healthcare more centrally (Cohn, 2009). Citizens feared what was there already and feared adding more complexity to the mix.

2.2.2 The Patient Protection and Affordable Care Act of 2010

A decade and a half later, buoyed by a cheerful electorate ready for the "hope" and "change" they had been promised in stump speech after stump speech, Obama pushed a revised national healthcare expansion plan through Congress. This presented additional government intervention into the healthcare system and expanded many government-funded programs – principally Medicaid. As Tow wrote, "The year-long process from President Barack Obama's inauguration in January 2009 to the enactment of the landmark bills in March 2010 were littered with deals, party-line tactics, and persuasive politics – strategies used to leverage positions, power, players, and perceptions." (Tow, 2011) These tactics got the legislation passed, but the rush to enact it has left policy and budget gaps across the government.

In March 2010, the Patient Protection and Affordable Care Act of 2010 (ACA for short) was passed and signed into law by Obama. The law enabled states to expand Medicaid coverage to millions, with the total cost of expansion paid by the federal government for the initial three years of the program, phasing back to 90% federal and 10% state funding by 2020. (Centers for Medicare and Medicaid Services, 2015)

While the verdict is still out, given the infancy of the current expansion program, much can be learned from previous initiatives to expand access to Medicaid and the early data points of the recent expansion. Currie and Gruber found positive effects of expansion for the medical treatments received by mothers during childbirth, with increased utilization by women with less education (Currie & Gruber, 2001). Benefits exist for the previously uninsured who now have access to care. Sommers found that Medicaid expansions were associated with a significant reduction in adjusted all-cause mortality, a relative decrease of 6.1%. (2012) A challenge lies in how to reach unserved populations without taxpayers taking responsibility for additional individuals who already have private insurance.

2.2.3 Medicaid Expansion and the Crowd-Out of Private Insurance

Card and Shore-Sheppard explored the failure of previous Medicaid expansion initiatives to reach low-income children, concluding that the failure of eligible individuals to register for insurance is a much more significant factor than crowd-out of private insurance. (Card & Shore-

Sheppard, 2004) However, using Survey of Income and Program Participation (SIPP) data, Blumberg found that 23% of the movement from private insurance to Medicaid was due to displacement. Gruber and Simon showed a significant private insurance crowd-out in the 1996-2002 expansion period. They found that "anti-crowd-out provisions in public expansions may have had the opposite effect, lowering take-up by the uninsured faster than they lower crowd-out of private insurance." (2008)

2.2.3 Medicaid Expansion and the Crowd-Out of Doctors

Garthwaite shows that doctors consistently spend less time with patients per visit to increase participation while decreasing work hours. (2012) Cunningham and May found that "Relatively low payment rates and high administrative costs are likely contributing to decreased involvement with Medicaid among physicians in solo and small group practices." (2006) Cunningham and Hadley found that reducing reimbursements for Medicaid patients would reduce doctor participation in the program. (2008) Medicaid pays doctors much less for their services than private insurance or self-pay patients. In reality, doctors whose demand is sufficient to allow them to opt out of providing care for Medicaid patients often will. Thus, Medicaid patients will gain access to care, but likely from a more limited set of healthcare providers than before ACA.

2.2.4 Medicaid Expansion Status

It is important to note that not all states have expanded their Medicaid programs to the extent federal legislation allows. Figure 3 depicts the status of the 50 states regarding expansion as of 2015. Noteworthy is that while 21 states have yet to adopt the provisions fully, many have taken steps to adopt some expansion provisions, easing into expanded coverage while maintaining a political stance against the law.

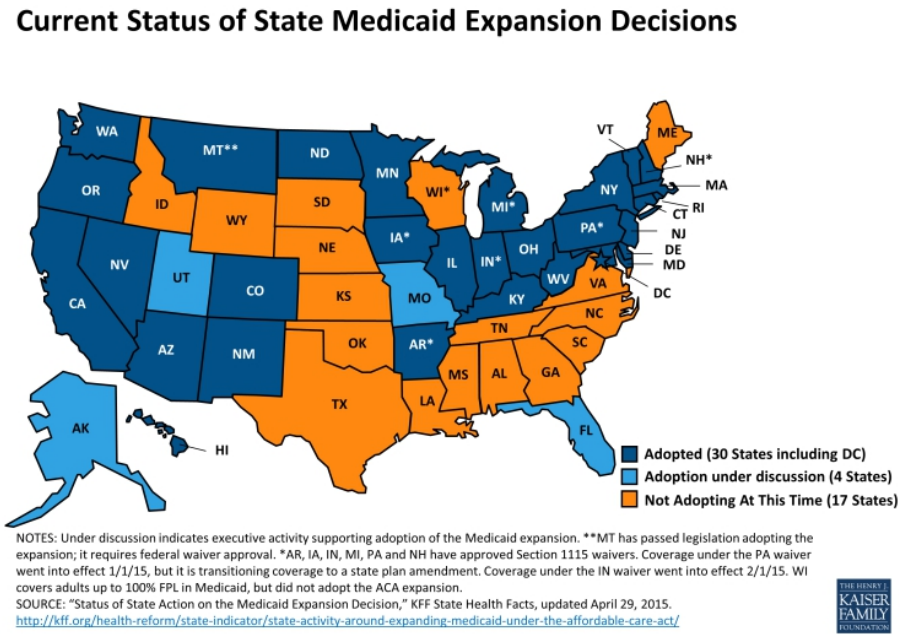


Figure 3 - Current Status of State Medicaid Expansion Decisions (Kaiser Commission on Medicaid and the Uninsured, 2015b)

An additional significant part of the Affordable Care Act was the requirement for the availability of Health Insurance Exchanges to allow for full-price and subsidized access to commercial insurance providers facilitated by a government-run online marketplace. Without a state system, these exchanges could be used by anyone not eligible for Medicaid and run by the state or the federal government. Figure 4 shows the current availability of Health Insurance Exchanges throughout the US and who operates the exchange in each state.

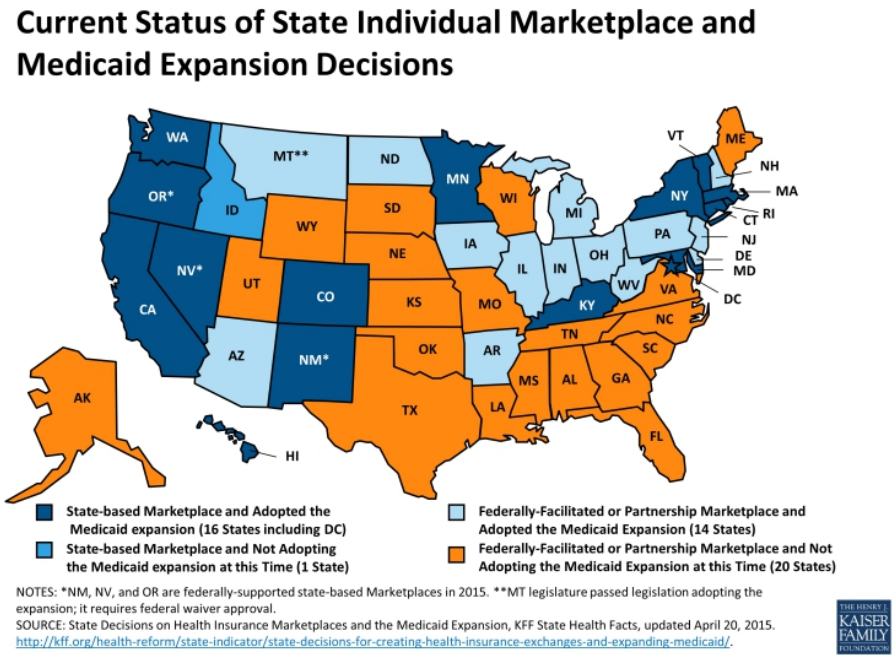


Figure 4 - Current Status of Health Insurance Marketplace and Medicaid Expansion Decisions (Kaiser Commission on Medicaid and the Uninsured, 2015a)

2.2.5 Cost of Medicaid Expansion

The Affordable Care Act and Medicaid expansion provisions would increase state Medicaid spending by $76 billion over 2013-2022 and federal spending by $952 billion. (Holahan, et al., 2012) While this is an enormous budget commitment for the governments, it [purposefully] puts states in an intractable position. Rose writes, “Whereas resources and history have served to reinforce the effects of partisanship and ideology, several countervailing forces – including public opinion, interest group pressure, budgetary considerations, and need – are pushing even the reddest states toward expansion.” (2015) In truth, too many special interests exist for states to refuse this grand overture of federal funds, which could create jobs in their states.

Glied and Ma discuss these significant investments of federal revenue in states. “The value of new federal funds flowing annually to states that choose to participate in the Medicaid expansion in 2022 will be, on

average, about 2.35 times as great as expected federal highway funds going to state governments in that year and over one-quarter as large as expected defense procurement contracts to states. No state would experience a positive flow of funds by rejecting the Medicaid expansion. Because the federal share of the Medicaid expansion is so much greater than the state share, taxpayers in nonparticipating states will nonetheless bear a significant share of the overall cost of the expansion through federal tax payments—and not enjoy any of the benefits." (Glied & Ma, 2013) Essentially, the citizens of all states will pay for the Medicaid expansion, whether their state accepts the funds to expand programs or not.

This begs the question: Do the increased tax revenues on providers and improving the general state healthcare ecosystem through the Medicaid expansion federal investment cover the expansion population's eventual 10% state costs? In a March 2015 case study, Dorn suggests that the early results of this question are favorable to states. Specifically, "Early evidence from interviews with budget officials in these case study states shows state savings and revenue gains with limited costs resulting from expansion, even as some potential fiscal gains have not yet been tracked" (Dorn et al., 2015). As the state share moves from 0% in 2015 to 10% by 2020, time will tell if the increased state tax revenues and lower proactive vs. reactive care costs can balance the significant impending state fiscal commitments to cover this population.

2.2.6 Non-Medicaid Provisions of the Affordable Care Act

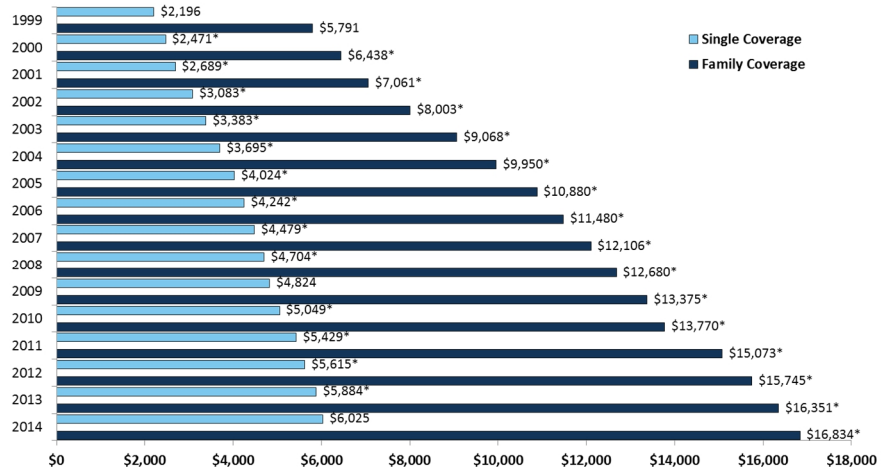
While Medicaid expansion was a large part of the ACA, the law's reach was broader and sweeping across the national health system. ACA mandates that all U.S. Citizens obtain and maintain health insurance coverage or face a fine. Section 1302 of the law requires that, to be considered a qualifying insurance plan, it must cover ten "Minimum Essential Health Benefits," including (ObamacareFacts.com, 2015):

1. Ambulatory patient services (Outpatient care). Care you receive without being admitted to a hospital, such as at a doctor's office, clinic, or same-day ("outpatient") surgery center. Also included in this category are home health services and hospice care (note: some plans may limit coverage to no more than 45 days).

2. Emergency Services (Trips to the emergency room). Care you receive for conditions that could lead to serious disability or death if not immediately treated, such as accidents or sudden illness. Typically, this is a trip to the emergency room, including ambulance transport. You cannot be penalized for going out-of-network or not having prior authorization.
3. Hospitalization (Treatment in the hospital for inpatient care). Care you receive as a hospital patient, including care from doctors, nurses, and other hospital staff, laboratory and other tests, medications you receive during your hospital stay, and room and board. Hospitalization coverage also includes surgeries, transplants, and care received in a skilled nursing facility, such as a nursing home that specializes in the care of the elderly (note: some plans may limit skilled nursing facility coverage to no more than 45 days).
4. Maternity and newborn care. Care that women receive during pregnancy (prenatal care), throughout labor, delivery, and post-delivery, and care for newborn babies.
5. Mental health services and addiction treatment. Inpatient and outpatient care provided to evaluate, diagnose, and treat a mental health condition or substance abuse disorder. This includes behavioral health treatment, counseling, and psychotherapy.
6. Prescription drugs. Medications that a doctor prescribes to treat an illness or condition. Examples include prescription antibiotics to treat an infection or medication used to treat an ongoing condition, such as high cholesterol. At least one prescription drug must be covered for each category and classification of federally approved drugs, however limitations do apply. Some prescription drugs can be excluded. “Over-the-counter” drugs are usually not covered even if a doctor writes you a prescription for them. Insurers may limit drugs they will cover, covering only generic versions of drugs where generics are available. Some medicines are excluded where a cheaper, equally effective medicine is available, or the insurer may impose “Step” requirements (expensive drugs can only be prescribed if the doctor has tried a cheaper alternative and found that it was not effective). Some expensive drugs will need special approval.

7. Rehabilitative services and devices – Rehabilitative services (help recovering skills, like speech therapy after a stroke) and habilitative services (help developing skills, like speech therapy for children) and devices to help you gain or recover mental and physical skills lost to injury, disability, or a chronic condition (this also includes devices needed for "habilitative reasons"). Plans must provide 30 visits each year for either physical or occupational therapy, or visits to the chiropractor. Plans must also cover 30 visits for speech therapy as well as 30 visits for cardiac or pulmonary rehab.
8. Laboratory services. Testing provided to help a doctor diagnose an injury, illness, or condition, or to monitor the effectiveness of a particular treatment. Some preventive screenings, such as breast cancer screenings and prostrate exams, are provided free of charge.
9. Preventive services, wellness services, and chronic disease treatment. This includes counseling, preventive care, such as physicals, immunizations, and screenings, like cancer screenings, designed to prevent or detect certain medical conditions. Also, care for chronic conditions, such as asthma and diabetes. (note: please see the full list of Preventive services for details on which services are covered.)
10. Pediatric services. Care provided to infants and children, including well-child visits and recommended vaccines and immunizations. Dental and vision care must be offered to children younger than 19. This includes two routine dental exams, an eye exam, and corrective lenses each year.

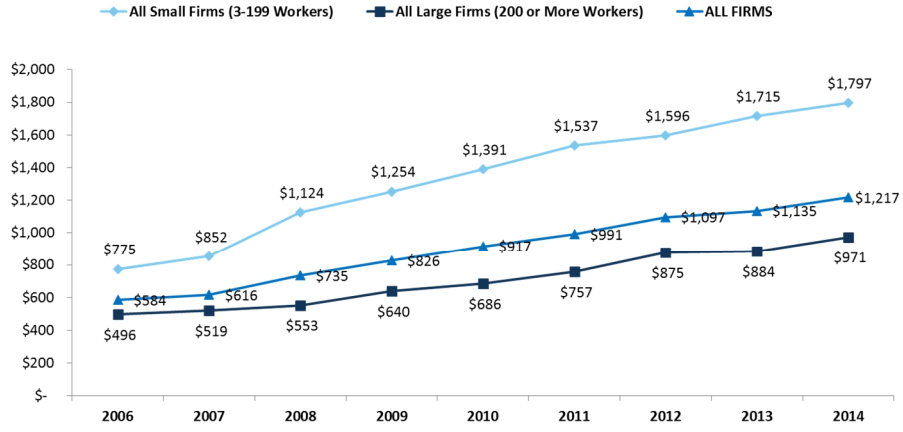
These provisions undoubtedly established a standard bar for insurance in the US. In setting this standard, most insurance offerings before ACA had to be amended to increase benefits and meet the law's requirements. This has led to significant increases in health insurance costs, as shown in both premiums (Figure 5) and deductibles (Figure 6).



* Estimate is statistically different from estimate for the previous year shown (p<.05).

SOURCE: Kaiser/HRET Survey of Employer-Sponsored Health Benefits, 1999-2014.

Figure 5 - Average Annual Premiums for Single and Family Coverage, 1999-201 (Kaiser Family Foundation, 2015)



NOTE: Note: Average general annual health plan deductibles for PPOs, POS plans, and HDHP/SOs are for in-network services.

SOURCE: Kaiser/HRET Survey of Employer-Sponsored Health Benefits, 2006-2014.

Figure 6 - Among Covered Workers with a General Annual Health Plan Deductible for Single Coverage, Average Deductible, by Firm Size, 2006-2014 (Kaiser Family Foundation, 2015)

2.3 Understanding the People, Organizations, and Governments that Comprise the U.S. Healthcare Ecosystem

Goldratt figured it out, writing, “Tell me how you measure me, and I will tell you how I will behave.” (1990). While he was not referring to the healthcare industry in any way, it could be the theme song for every actor in the healthcare system. Kaplan states, “A short-term perspective characterizes the healthcare system. The government has essentially an election-to-election planning horizon, and the enterprises are mostly driven by short-term financial and profit objective” (2011).

Figure 7 provides a more simplified relational view of actors in the US healthcare system than The New Republic map. The following subsections describe each of these actors, focusing on the US Medicaid system and the characteristics of each actor relevant to healthcare fraud, waste, and abuse.

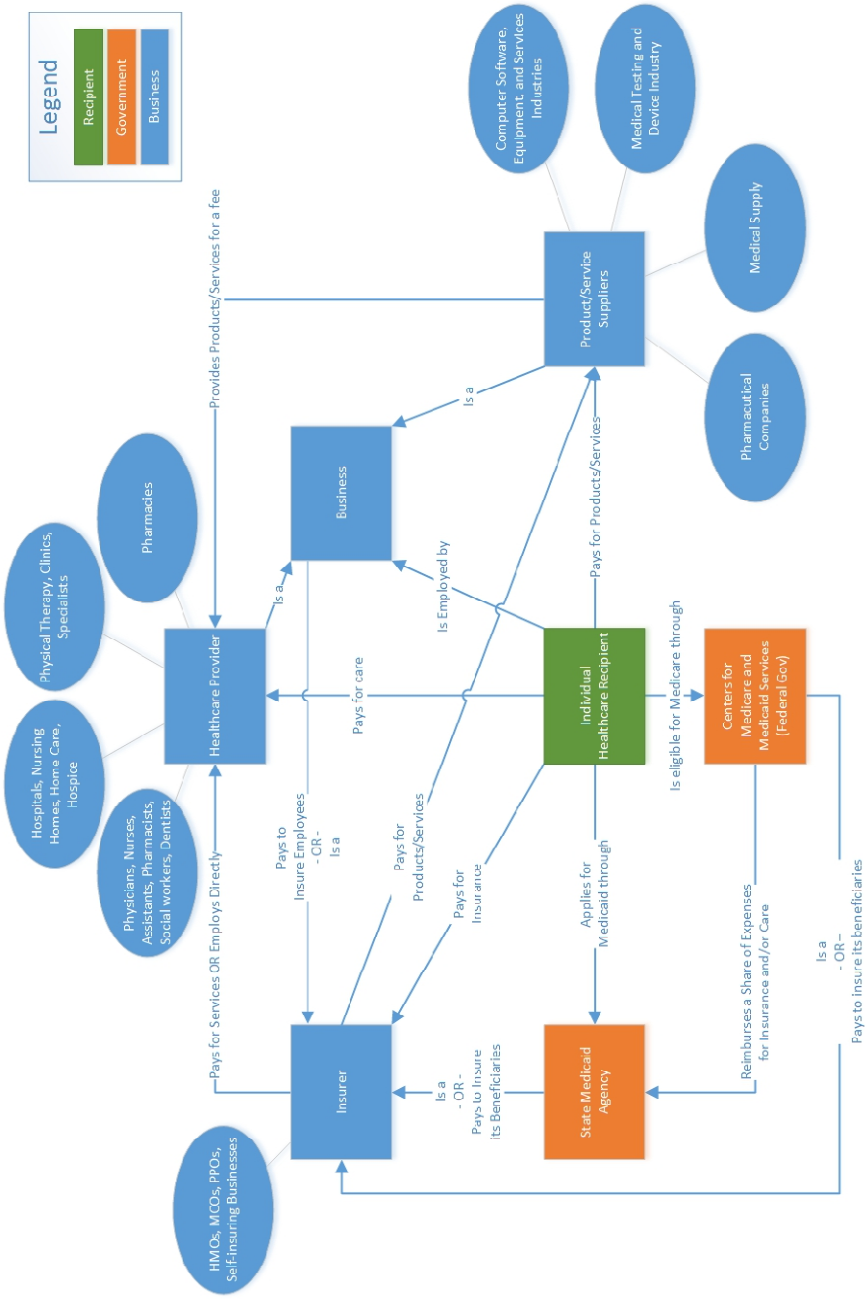


Figure 7 - Actors and Relationships in the US Healthcare System

2.3.1 Individual Healthcare Recipients

The individual is the basis for the system, the person who receives care and is ultimately responsible for obtaining and paying for it.

All US citizens must obtain health insurance coverage or pay a fine as part of the Affordable Care Act. Insurance is typically provided through a "group plan" such as through an individual's employer, with the employee paying some share of the cost, directly through open insurance markets, or through a government program such as Medicaid or Medicare. The individual is responsible for seeking out their insurance options and obtaining insurance.

As individuals, we obtain care from doctors, hospitals, therapists, dentists, etc., get drugs at pharmacies, buy medical equipment such as orthopedic braces from durable medical equipment suppliers, and utilize services such as diagnostic testing. To the extent these services are partially or fully covered by insurance, these providers bill one's insurance policy and then charge the balance to the patient.

Kickback, pay-for-play, and eligibility fraud scenarios are possible at the individual level (Thornton et al., 2015). Unfortunately, due to asymmetric information caused by the complex nature of the current system and privacy laws, honest patients often do not know they are being exploited for fraudulent activities.

2.3.2 Businesses (Employers)

Across the US, under the Affordable Care Act, businesses of all types must offer health insurance to all their employees working at least 30 hours per week or face fines of $2,000 per FTE beyond the first 30 employees. Coverage offered to employees can cost up to 9.5% of employee household income and must have an average cost sharing of at least 60% paid by the employer. (Patient Protection and Affordable Care Act, 2010) Employers with over 200 FTE must automatically enroll new full-time hires and provide a manual opt-out to employees. As shown in Figure 8, most individuals are covered by employer-sponsored plans.

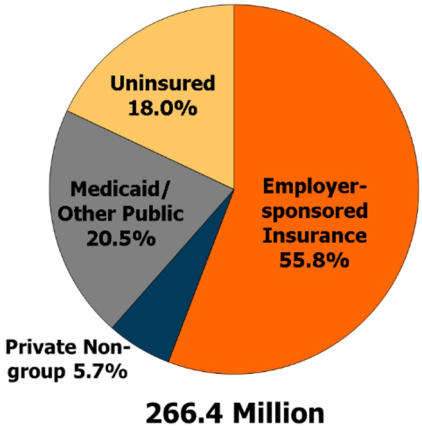


Figure 8 – 2011 Health Insurance Coverage of the Nonelderly Population (Kaiser Commission on Medicaid and the Uninsured, 2012)

2.3.3 US Federal Government & CMS

In the United States, the Centers for Medicare & Medicaid Services (CMS) is a federal agency within the Department of Health and Human Services responsible for the administration of many public health programs, including Medicare, ACA standards implementation, and working with states, Medicaid, and the State Children's Health Insurance Program (SCHIP). CMS pays regional claim processors and insurers directly to administer the Medicare program based on federal program policies.

Medicaid is administered by each state, with CMS providing cost-sharing on both the claims payment and the development and operations of state healthcare IT systems. Much like federal highway funding in the US, this cost-sharing comes with many strings attached and exists as a fiscal mechanism for the federal government to direct state health policy and compliance with national standards on the IT front.

From a Medicaid fraud, waste, and abuse perspective, CMS sets standards and works to contain costs. The Deficit Reduction Act of 2005 created the Medicaid Integrity Program, enshrined in 42 U.S.C. §1396u-6. This program created federal review and audit of providers, identification and recovery of overpayment, and education resources to assist states with program integrity efforts. It created federal staffing and contracts to go after fraud in Medicaid. However, Medicaid is still a state-run program with state-

specific policies, data frameworks, and politics. Homogeneous national efforts are challenging, at best.

2.3.3 State Governments and Medicaid

State governments oversee Medicaid programs for their states, primarily servicing families and individuals with low income and limited resources. Each state sets policy for who is eligible to receive benefits and what the benefits are, in compliance with federal laws and policies determining federal cost-share. While states are not required to participate in Medicaid, all currently do, as it serves a pressing underserved social need and provides significant financial resources to the state/local government and the healthcare industry.

The Social Security Amendments of 1965 created Medicaid, and it has since been continually evolving with the political ebbs and flows of Washington and the states. In 2010, the Affordable Care Act sought to significantly expand Medicaid eligibility nationally, fully funding an eligibility threshold of income up to 133% of the poverty line for a limited time. In National Federation of Independent Business v. Sebelius (*National Federation of Independent Business v. Sebelius*, 2012), the Supreme Court ruled that states did not have to implement the federal 133% standard to continue receiving previous levels of Medicaid funding. Many states have chosen to block "Medicaid Expansion" and continue with pre-ACA eligibility standards and funding models.

State programs vary from pure fee-for-service to fully managed-care environments. In some states, the claims processing is administered by the state itself. In others, the processing is contracted, or the total liability is outsourced to insurance companies on a capitated basis.

Like any health insurer, the state must maintain a network that addresses its population. States must make trade-offs between cost, quality, and access as they design and manage their programs. In its review of peer-reviewed studies on managed care in Medicaid (Sparer, 2012), Sparer discussed the lack of evidence supporting a singular national approach to Medicaid managed care and the importance of local considerations in success stories to date. Specifically, he suggested:

- Policymakers may want to be far more cautious and conservative in their estimates of the likely benefits of Medicaid-managed care. They must carefully consider the trade-offs between costs, access, and quality. For example, programs that improve access and quality are not likely to save money, especially in a program that is already relatively low-cost.
- Focusing managed care on cost savings could reduce access or quality. In other words, developing initiatives that simultaneously improve access and quality while reducing costs is difficult. Managed care may be the next step for Medicaid, but it is not a magical panacea.
- There is a clear need for more and better research on the impact of Medicaid-managed care on costs, access, and quality, including research focusing on individual states and national data. This is especially true for the emerging programs for high-cost beneficiaries.

States are at the epicenter of administrating Medicaid but are caught between the many stakeholders in the healthcare value system and politically.

From an anti-fraud perspective, states have many disincentives to take up the fight. Typically, fraud, waste, and abuse are found post-payment and are challenging to recover. Regardless of whether a recovery is made, the state must pay back the federal cost-share, further impacting the state budget beyond the original payment. The political ramifications of audits can also be painful and less than desirable for elected and appointed officials. Discovering fraud, waste, or abuse, especially post-payment, means someone will be unhappy.

2.3.4 Insurers

Insurers receive funding to take on the liability of servicing a patient and provider population. They must maintain provider networks to provide access to quality care throughout the state. They must provide eligibility determinations in a timely manner. They must pay providers quickly and accurately. They should seek to provide quality care to their beneficiary population and to reduce costs, where possible.

Under many of the same pressures as the states but with the inherent leadership goal of corporate profit, insurers have more latitude in performing the cost vs. access vs. quality tradeoffs than the states themselves. However, one would expect corporate entities to be more competitive than in practice.

The purchasers supply the funds. These include individual healthcare consumers, businesses that pay for their employees' health insurance, and the government, which pays for care through public programs such as Medicare and Medicaid. All healthcare purchasers are ultimately individuals, as individuals finance businesses by purchasing their products and fund the government by paying taxes. Nonetheless, businesses and the government are essential as the nation's organized healthcare purchasers.

The insurers receive money from the purchasers and reimburse the providers. Traditional insurers take money from purchasers (individuals or businesses), assume risk, and pay providers when policyholders require medical care. However, some insurers are the same as purchasers; the government can be viewed as an insurer or purchaser in the Medicare and Medicaid programs, and businesses that self-insure their employees can similarly occupy both roles. (In previous chapters, the term “payer” was used to refer to both purchasers and insurers.)

2.3.5 Providers

The providers, including hospitals, physicians, nurses, nurse practitioners, physician assistants, pharmacists, social workers, nursing homes, home care agencies, and pharmacies, provide the care. While health maintenance organizations (HMOs) are generally insurers, some are also providers, owning hospitals and employing physicians. Providers bill insurers and patients for services rendered fee-for-service or capitated.

When a provider participates in Medicaid, the provider agrees to reimbursement by the state and submits claims for payment directly to the state or managed care entity. States operate claims processing systems that perform various prepayment checks and edits to inspect the claim’s legitimacy. Edits and audits verify information with honest providers in mind, but they are not designed to detect fraud schemes of any depth (Sparrow, 2000). These systems cannot verify whether the service was

provided as claimed, the diagnosis is correct, or whether the patient is even aware of the services.

Traditionally, providers have received better reimbursement rates from private payers and private health insurers, with Medicare and Medicaid sometimes paying significantly less on a per-procedure basis. As such, many providers elect not to participate in Medicare and Medicaid programs, instead only serving private payers. With the Medicaid expansion in ACA, even more patients were hoisted into an already congested network of physicians and practices serving the Medicaid populations. At what point does doctor crowd-out leave the system in a state where quality of care is unacceptable? Providers are the least incentivized actors to contain costs or report violations. Providers are the initiating actors for billing healthcare payers, and, as such, unscrupulous ones can quickly become the nexus for fraud schemes.

On the flip side, in a report entitled "Tick, Tick, BOOM: CMS's Proposed 60-Day Rule Would Create Intense Time Pressure for Providers to Identify, Report, and Return Overpayments," Deeringer discusses the impacts of part of the ACA legislation that required providers pay back Medicaid within 60 days of the identification of an overpayment (2012). "Overpayment" is broadly construed, as is "identification," and the impact on providers from an administrative and legal compliance perspective is quite significant. Will such changes reduce fraud or drive more providers out of the networks, further eroding Medicaid's quality and access to care? Policymakers face many double-edged swords when crafting change in a complex and interrelated system.

2.3.6 Product / Service Suppliers

The pharmaceutical, medical supply, and computer industries manufacture equipment, supplies, and medications providers use to treat patients. Significant institutional inertia exists in these industries due to public safety and compliance requirements with the Federal Drug Administration (FDA) and CMS. These are some of the largest entities in the healthcare industry, from the pharmaceutical sector to durable medical equipment (DME) to electronic health record (EHR) systems, with billions in revenue annually. These actors are incentivized to push their products. As such, kickback

schemes, bribery, and similar scenarios have been played out at the provider, patient, and regulatory levels (Thornton et al., 2015).

2.4 Medicaid Claims Process

(adapted from (Travaille et al., 2011)*)*

When a provider participates in Medicaid, the provider agrees to the reimbursement rates set by the state and submits claims for payment directly to the state's Medicaid agency. If the provider is not participating in Medicaid, the provider sends the patient the bill, which they must pay before requesting reimbursement for partial payment from Medicaid. In both scenarios, the state Medicaid agency processes the claim and sends an explanation of benefits (EOB) to the beneficiary. An EOB is an automatically generated overview of the provided services and corresponding codes and costs.

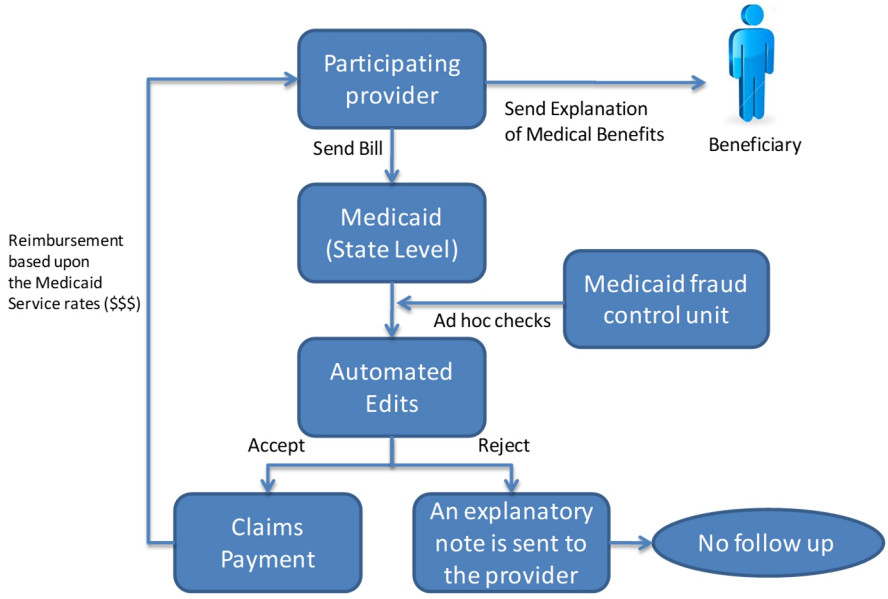


Figure 9 - Provider Claim Submission to Medicaid

Every state is responsible for organizing, governing, and operating its Medicaid program. The states process claims using software that differs from state to state. The software performs several prepayment checks and

edits to verify that the claim is legitimate. Sparrow (Sparrow, 2000) provides some examples of the automated audits:

- Have the mandatory fields been filled in?
- Do the procedure codes match the diagnosis?
- Is the pricing in range with the set boundaries for the service or procedure?
- Has the claim been submitted and paid already (duplicate claims)?

The edits and audits are designed to verify the information with honest providers in mind. However, the system lacks effective fraud detection mechanisms (Sparrow, 2000). The systems need to verify that the service was provided as claimed, if the diagnosis is correct, or if the patient is aware of the claimed services, as they do not possess appropriate, verifiable information. In addition, when a claim is rejected, there is no follow-up investigation as to why an invalid claim was submitted (Sparrow, 2000). Instead of vetting these claims, the system sends an explanation to the provider with the reason why the claim was rejected. Thus, instead of flagging what could be fraudulent activity, the system teaches potential fraudsters about the system's billing rules and edits.

EOBs, while well-intentioned, provide minimal protection against fraud in their current form (Sparrow, 2000). The beneficiary has little to no financial incentive to pay attention to them. Recipients do not understand the complex computer-generated forms and billing codes. Fraudulent providers have even incentivized beneficiaries not to read them, including paying $5 per unopened envelope given back to the provider. In addition, many fraud schemes deliberately target vulnerable populations that cannot open or understand the EOB or are given kickbacks from the provider not to complain (Kelley, 2009).

2.5 A Framework for Describing the Actors in Medicaid

(adapted from (Thornton et al., 2013)*)*

Distilling much of the narrative and policy context of Section 2.3, Table 1 provides an analysis of the primary Medicaid actors that guides the proposed antifraud framework design.

	Patient	Provider	State Medicaid Agency / Insurer	CMS (Federal)
Roles	Enroll in Medicaid. Receive care. Receive EOB.	Enroll with Medicaid. Provide care. Submit claims. Receive payment.	Sets (comparatively low) reimbursement rates. Enroll beneficiaries and providers. Pay legitimate claims. Prosecute fraudulent claims. Provide EOB to patient.	Pay state matching funds on claims. Ensure state matching funds are well-spent.
Capabilities	Could commit, conspire to commit, or report fraud.	Could commit, conspire to commit, or report fraud.	Can analyze patients, providers, and claims within its jurisdiction.	Could simplify data sharing across states. Could provide common tools for states to use for detecting fraud.
Characteristics	Wants to receive quality care at low out-of-pocket costs. Insurance identity theft has little direct impact on patient.	Desire quick reimbursement for services rendered. Unhappy with low reimbursement rates. Will opt-out of participation with significant burdens. Bad actors can sap millions quickly.	Want to reduce fraud / waste / abuse. Tight state budgets limit operational dollars available to combat fraud. Afraid of discovering unrecoverable fraud, as the state is responsible for both loss and to reimburse federal matching funds. Afraid of impositions on providers pushing them out of the system, reducing access to care.	Want to reduce fraud / waste / abuse. Afraid of impositions on providers that may push them out of the system, reducing access to care. Afraid of impositions on states that may reduce cooperation with federal initiatives such as ACA.
Fraud / Anti-Fraud Strategies	Could: receive kickbacks, sell credentials, receive free services, or look the other way.	Could: phantom bill, up code, unbundle, miscode, bribe patients, perform unnecessary services, or refer patients to collusive providers. Could also sell credentials for billing and/or be extorted by organized crime.	Checks claims against known 'edits'. Performs some data analysis of state claims paid as a source of audits. Audits providers for reasonableness and accuracy. Prosecutes blatant fraud through the court system. Excludes proven fraudulent providers.	Aggregates data at a national level for analysis. Supports focused state and interstate collaborations, auditing providers with the state and providing funding for specific anti-fraud collaboration efforts. Provides training to state staff. Prosecutes blatant fraud legally. Excludes fraudulent providers.

	Patient	Provider	State Medicaid Agency / Insurer	CMS (Federal)
Structure /	Millions of independent actors.	Millions of independent actors.	Struggle between pleasing providers and finding fraud. Program integrity is usually in a separate silo away from payment and enrollment operations.	Struggle between pleasing providers and finding fraud. Program integrity is usually in a separate silo away from payment and enrollment operations.
Processes	Receive services. EOBs are sent to the patient by the insurer.	Enroll in Medicaid. Provide care. Bill for care. Respond to audits. Maintain records.	Provider and beneficiary enrollment. Claims payment process. Claims data extract process for CMS. Provider audit processes. Audit findings extrapolation process.	Medicare provider and beneficiary enrollment. State data quality processes. State audit support and collaboration processes.

Table 1 - Medicaid Environment Overview

2.6 Conclusions

The U.S. healthcare system, particularly Medicaid, is intricate and has evolved over many years, influenced by various political agendas. The complex relationships within this system make it challenging to directly apply traditional fraud-fighting methods that have proven successful in other sectors (Travaille et al., 2011). Asymmetric information hinders the ability of individual participants in the value network to unlock their potential fully and to prevent or mitigate fraud. To enhance the quality and accessibility of care while simultaneously reducing total costs—including those associated with fraud, waste, and abuse—innovative tools and strategies are essential.

3

Chapter 3: Defining the Types of Fraud in Healthcare

Adapted from:

Dallas Thornton, Michel Brinkhuis, Chintan Amrit, Robin Aly, "Categorizing and Describing the Types of Fraud in Healthcare," in Procedia Computer Science, Conference on Health and Social Care Information Systems and Technologies, Volume 64, 2015, Pages 713–720.

Chapter 3: Defining the Types of Fraud in Healthcare

3.1 Introduction

This chapter delves into the insights garnered from healthcare fraud detection through a comprehensive literature review of published works related to healthcare fraud. Given the rapidly evolving nature of this field, I aim to identify which fraud schemes have been documented and investigated. Section 3.2 outlines the methodology used for the review. Section 3.3 presents the findings, highlighting specific fraud scheme types and analytical methods in contemporary literature. Lastly, Section 3.4 offers conclusions and suggests potential avenues for future research.

3.2 Methodology

In this chapter, I aimed to conduct a comprehensive literature review to identify various health insurance fraud schemes. I employed a structured literature review methodology, as Webster and Watson (2002) outlined, utilizing a concept matrix to guide the process. The following steps were taken:

- Keyword Identification: Initiated the review by establishing a set of relevant keywords.
- Refinement of Keywords: Adjusted the initial set based on the results obtained, ensuring relevance and precision.
- Initial Filtering: A preliminary screening was conducted based on titles, eliminating articles in unsupported languages and those unrelated to the topic.
- Abstract Review: The selection was refined by reviewing abstracts and discarding irrelevant articles.
- Detailed Article Review: Conducted an in-depth examination of the remaining articles to identify key concepts and details.

This literature study aimed to find literature related to types of health insurance fraud. Fraud related to health, healthcare, health insurance, or the Medicaid program is relevant to this research. The terms “health,” “healthcare,” and “medical insurance” cover a broad spectrum of potentially interesting articles. The query below was utilized for baseline search results.

TITLE ((Medicaid OR "health" OR “healthcare” OR "medical insurance") AND fraud)

Figure 10 - Search Query Used

This query was then run through two prominent scientific search engines, Scopus and Web of Science, encompassing various technical and medical articles. Web of Science also includes access to PubMed, a crucial database for biomedical literature.

Several filters were applied during the search to refine the results. These included a language filter, ensuring only English-written articles were considered, and excluding citations and patents, focusing solely on journal articles and scientific papers.

The search yielded 152 documents from Scopus and 248 from Web of Science. All results were collated in Microsoft Excel, providing a comprehensive overview of all authors, titles, and abstracts. Following this, duplicates were identified and removed based on titles and authors, resulting in a unique 252 articles.

Upon initial review, it was evident that many articles were not directly related to healthcare fraud. A more refined selection process was then undertaken, evaluating the relevance of each article based on its title and abstract. After this rigorous screening, 183 articles were deemed irrelevant or inaccessible due to non-publication online or restrictions in subscription services. This process ultimately left a pertinent set of 69 articles.

3.3 Fraud Types Described in Literature

Upon an extensive evaluation of 69 scholarly works, we selected 27 articles comprehensively describing various types of fraud in the healthcare sector. It is noteworthy that several articles address more than one type of fraud. The following sections detail 18 types of fraud identified in the literature, with the number of articles discussing each kind illustrated in Figure 10.

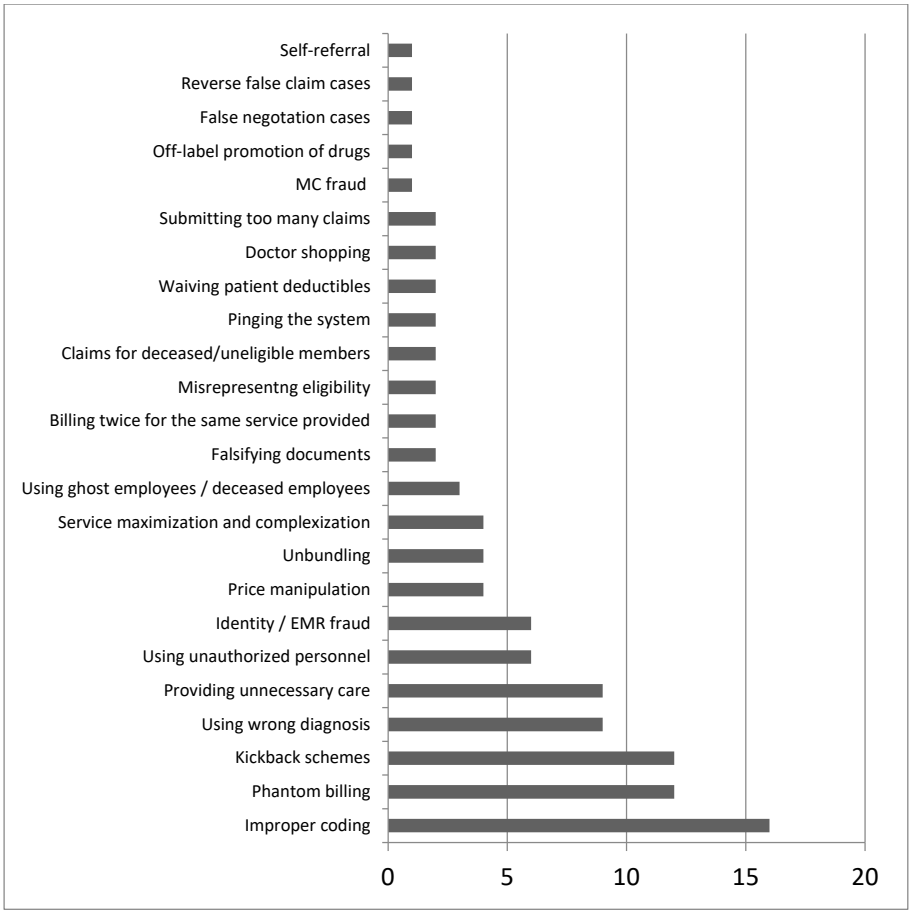


Figure 10 - Incidence of health insurance fraud types in literature.

3.3.1 Kickback Schemes

Kickback schemes are prevalent and widely discussed in healthcare fraud literature. These schemes can manifest in various forms, but a kickback is a payment made to an individual for facilitating a transaction or appointment. For example, a pharmacist may opt for a particular brand of medication, influenced by financial incentives from a pharmaceutical company (Rabecs, 2006). Additionally, physicians might engage in unethical practices by writing prescriptions in exchange for monetary benefits, contributing to the illegal drug trade (Morris, 2009).

3.3.2 Self-Referral

Rashidian (2012) defines self-referrals as “referring the patients to a clinic, diagnostic service, hospital, etc., with which the referring physician has a financial relationship.” This might involve a kickback scheme if the referred-to party pays a commission back to the physician, but other financial relationships are conceivable. For example, many physician groups and hospitals are sustaining through growth. While some economies of scale are achievable through growth, referrals within the same financial organization are becoming routine and accepted practices that typically elude significant scrutiny.

3.3.3 Doctor Shopping

If feigning pain or bribing a doctor does not work, a drug-seeking person may look for another doctor who will provide the desired prescriptions. A patient can easily visit multiple doctors and locations to obtain prescriptions (often multiple times). Carlson (Carlson, 2013) refers to a study by the US Government Accountability Office that found that in 2011, about 600 patients in the Medicare program filled prescriptions from more than 20 doctors each.

3.3.4 Identity Fraud

Identity fraud may happen when an uninsured individual assumes the identity of a person with insurance coverage to obtain services or to hide a specific illness (Marijn G.A. Plomp & Jan H.A.M. Grijpink, 2011). They discuss that the healthcare services eventually provided to the person ‘lending’ their identity could be adversely affected since their health records contain unrelated and potentially contrary information.

Identity theft can also happen without the owner of the identity knowing. Dube (Dube, J. F., 2011) mentions identity theft by foreign gangs that have scammed federal authorities for millions of dollars.

3.3.5 Fraud by Pharmaceutical Companies

Sparrow (2008) describes pharmaceutical abuses beyond the kickback schemes mentioned above. Specifically, off-label promotion of drugs involves the marketing of medicines for uses, which the Food and Drug Administration does not approve. Illegal price manipulation and inflation in

collusion with downstream data providers or other pharmaceutical companies have been shown on multiple occasions.

3.3.6 Device and Services Price Manipulation

Similar to pharmaceutical companies, but usually on a smaller, more regional scale, medical equipment or health services providers can manipulate prices for certain groups of clients (Sparrow, 2008). They may increase prices directly if they know Medicaid will pay varying service rates. Alternatively, they may move across the street to the next zip code, from which they can bill at a higher rate.

3.3.7 Improper Coding and Upcoding

Improper coding, sometimes called upcoding, is among the most discussed and prevalent fraud topics. Agrawal (Agrawal et al., 2013) describes upcoding as "billing for a more expensive service or procedure than the one performed." He also describes improper coding, which he differentiates as due to an administrative error versus a malicious attempt to increase revenue.

3.3.8 Unbundling

Unbundling means creating separate claims for actions that are part of one procedure (Rashidian et al., 2012). Unbundled claims typically result in higher charges for single services versus discounted services because they are interrelated and bundled. Unbundling may be seen as a part of improper coding, but multiple authors mention unbundling as a separate form of fraud. Today, software such as Grouper looks for unbundling and will either reject unbundled claims or "re-bundle" the claims and adjust the bill to pay for the combined procedure code.

3.3.9 Submitting Duplicate Bills

Care providers can also try to submit the same claim multiple times to get paid twice for performing one action. Byrd (2013) describes double billing as "billing multiple times for the same service."

3.3.10 Billing for Services Not Provided

With double billing, at least care is provided to a patient. With billing for services not provided, claims are submitted for healthcare services that have not been provided or for medicines or medical devices that have not

been delivered to the patient. This concept is called *phantom billing* (Rashidian et al., 2012). One of the examples mentioned by Stanton (2001) described providers that submit so many claims in one day that it is not physically possible (or at least highly unlikely) to help so many patients. To overcome this minor obstacle, Brooks (2012) describes the new practice of ghost employees: fake employees on the health providers' payroll that do not exist. Thornton (2013) describes multidimensional data models centered around providers and provider groups that can be utilized to highlight excessive billing at the provider and provider group models.

Related to this method of fraud is submitting false claims to the systems to discover how to get a false claim approved. Since claims are mostly automatically processed, knowing the thresholds of the claim handling systems allows one to submit claims for services not provided that do not trigger monitoring systems (Morris, 2009). There are several ways these types of schemes are found out. Accurate patient information is needed to submit and be paid for false claims. Sometimes, a false claim is submitted for a patient no longer alive. Even more blatant – sometimes, a claim is submitted using the identity of a deceased physician (Morris, 2009).

3.3.11 Providing Medically Unnecessary Care

More healthcare may also be provided than was needed to heal the patient, thus providing unnecessary care. Sometimes, certificates are falsified (Rashidian et al., 2012) to show the medical necessity of specific actions to justify payments. Morris(Morris, 2009) also describes maximizing the number of services and claims. The fee-for-service model means that physicians get paid based on the services they provide – maximizing the number of services means maximizing their pay. Outlier detection techniques have shown promise in detecting providers that differ from their peer groups (Thornton et al., 2014).

Other examples of unnecessary care include 'Rolling labs,' which administer tests provided by healthcare providers that temporarily visit shopping centers or retirement houses (Borca, G., 2001). These are simple tests but are billed as expensive procedures to insurance programs. Furthermore, sometimes, care providers use unproven or unnecessary treatments with questionable potential patient outcomes.

3.3.12 False Negotiation

False negotiation cases mentioned by Doan (2011) are cases that arise from situations in which a healthcare provider makes false statements to induce the government to enter into a contract for services or supplies. Sometimes, this is also referred to as *frauds-in-the-inducement*.

3.3.13 Using the Wrong Diagnosis

Claims are submitted for a service provided based on a stated diagnosis. These diagnoses can also be manipulated -- a patient can get a specific diagnosis when that diagnosis is reflective of the individual's condition (Ogunbanjo et al., 2014). This can be done to justify fraudulently prescribing certain medicines to a patient.

3.3.14 Billing for Services Rendered by Unqualified Personnel

People can provide care without the credentials to perform that kind of care (Rashidian et al., 2012). An example is when an intern or anyone training in the medical field provides care that a physician bills for and which the intern is uncertified to perform or unqualified to bill.

3.3.15 Lying about Eligibility

Patients can lie about their situation when they visit a pharmacist or a physician. They can, for example, claim exemption from prescription charges when they are not exempt (Rashidian et al., 2012), or they can misrepresent information about their dependents to get insurance coverage (James D. Byrd Jr. et al., 2013).

3.3.16 Reverse False Claims

False claims paid by an insurance program result in a provider receiving money from the insurer. *Reverse false claims* represent situations where a care provider owes money to the government and does not pay it back on time (Borca, G., 2001).

3.3.17 Managed Care Fraud

Managed care, as opposed to fee-for-service, is taking on a growing proportion of the US health insurance market. Within Medicaid, Managed Care Organizations (MCOs) now cover most patients. This insurance mechanism theoretically passes risk from the primary payer to an intermediary insurer, which is paid at a capitated rate for the population

they insure. Doctors participate at risk, taking a capitated rate for their patients for particular services or in a fee-for-specific-services arrangement. These changed incentives provide for new areas of fraud, as Sparrow (2008) mentioned, including denial of services to patients, providing substandard care, and creating logistical and administrative obstacles for patients to receive the care they need.

3.3.18 Waiving Co-Payments

Insurance plans can require co-payments for certain services to incentivize patients to make appropriate cost-minded decisions in their healthcare. Freeman and Loavenbruck (2001) discuss healthcare providers waiving co-payments or deductibles, removing these incentives, and violating their participation agreement with the insurer.

3.4 Conclusions

This systematic literature review evaluates health insurance fraud types across published works. Much work has been done in this space in recent years, yet much work remains. Sun Tzu (Sunzi & Giles, 2005) wrote, “Know your enemy and know yourself, find naught in fear for 100 battles. Know yourself but not your enemy, find level of loss and victory. Know thy enemy but not yourself, wallow in defeat every time.” Healthcare fraud is an evolving field, with new schemes emerging regularly. In this review, the enemy is discussed and described, hoping to understand better the types of fraud that plague healthcare today. To succeed in combatting fraud, one must fundamentally understand healthcare systems and how data mining and analytic techniques can be applied within them to detect fraudulent activity.

Extending the current literature review, the selected 69 works can be categorized into two categories: health insurance fraud types and methods for detecting health insurance fraud. Figure 11 shows the number of works covering each technique used for fraud detection.

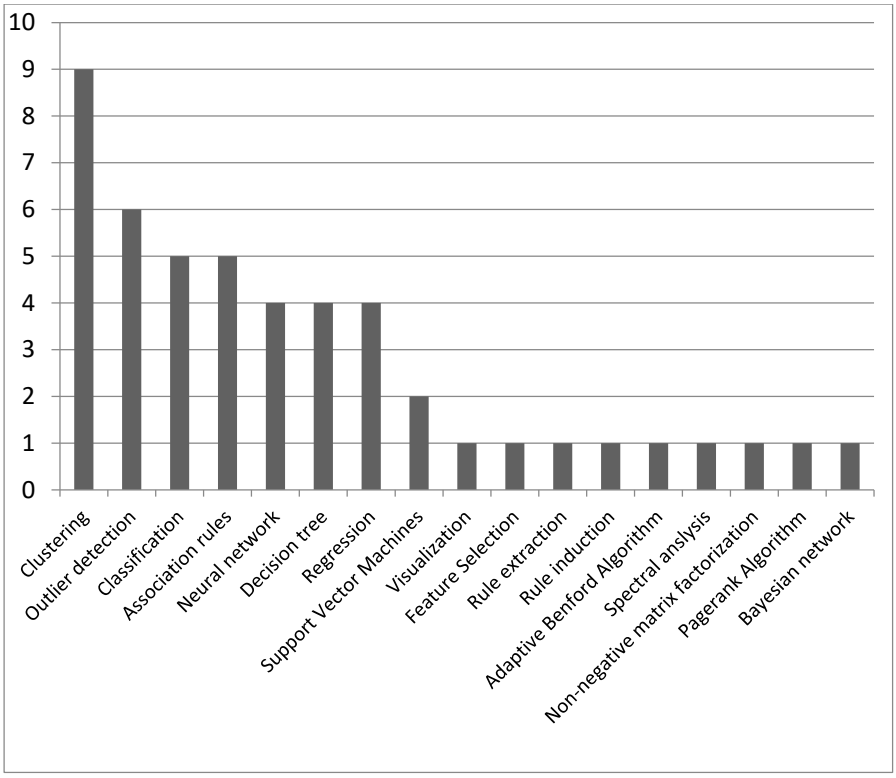


Figure 11 - Incidence of Different Health Insurance Fraud Detection Methods in Literature.

Future research will describe how these techniques are being used to combat healthcare fraud and develop models that map these techniques to fraud types and tool frameworks. The fight against fraud in healthcare will be an ongoing struggle. By knowing our enemy and employing an ever-increasing arsenal of technologies and analytical tools at our disposal, we can make continual progress in improving the state of the industry and combatting healthcare fraud.

4

Chapter 4: Fraud Detection Methods in Other Industries

Adapted from:

Peter Travaille, Roland M. Mueller, Dallas Thornton, Jos van Hillegersberg, Electronic Fraud Detection in the U.S. Medicaid Healthcare Program: Lessons Learned from Other Industries, AMCIS Proceedings, Association for Information Systems, (2011).

Chapter 4: Fraud Detection Methods in Other Industries

4.1 Introduction

Health insurance fraud and abuse are challenging to discover because of asymmetric information between the insurer, beneficiary, and provider (Derrig, 2002). Investigating how electronic fraud detection techniques have been successfully employed in analogous sectors can yield valuable insights. Industries such as insurance, telecommunications, and particularly the credit card sector deem fraud detection critical for maintaining sustainability and competitiveness.

This chapter offers a systematic literature review focusing on applying electronic fraud detection techniques across these comparable industries. Section 4.3 delves into various fraud schemes that have been unearthed in the past. Section 4.4 provides an extensive analysis of pertinent fraud detection methodologies, supplemented by references to key published works in the field. Finally, Section 4.5 explores lessons from these related industries, evaluating the pros, cons, and limitations of the discussed fraud detection methods applied to the Medicaid program.

4.2 Methodology

The foundation of this research is a systematic literature review. The following databases have been reviewed to systematically review appropriate scientific journals, with an initial focus on the top 25 information systems journals (Schwartz & Russo, 2004): Web of Science, Scopus, PiCarta, and Google Scholar.

Figure 12 shows the systematic literature review process, with a top-down search driven by the keywords and the bottom-up search approach using forward and backward citation analysis. Using this methodology, relevant disciplines such as finance, telecommunications, healthcare, and computer intrusion detection (see Table 5) have been included in the review. Exclusion criteria were articles older than 15 years and papers focusing on algorithmic data mining without an emphasis on or application to fraud detection.

Keywords:

- Electronic Fraud Detection
- Health Care Fraud
- Fraud Detection
- Data Mining
- Supervised Data Mining
- Unsupervised Data Mining
- Credit Card Fraud
- Insurance Fraud
- Statistical Fraud Detection
- Fraud and IT
- Anomaly Detection

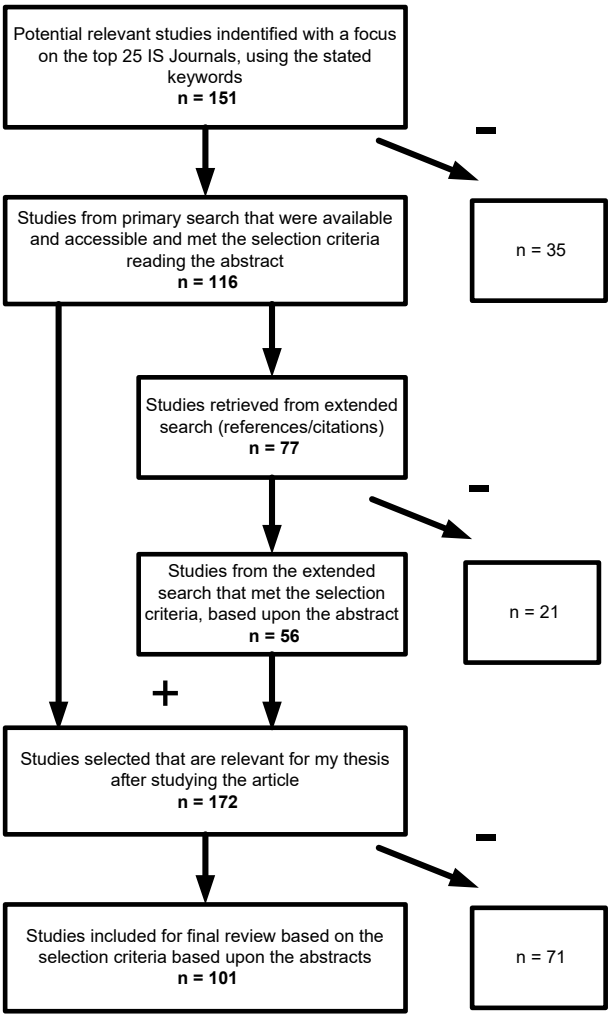


Figure 12 - Systematic Literature Review

4.3 Healthcare Fraud Types

4.3.1 Definition of Fraud and Abuse

The terms fraud, waste, and abuse, as used in literature, encompass a broad spectrum of conduct, ranging from intentional misrepresentation of services provided to inadequate documentation of provided care (Hyman, 2001). Waste and unnecessary services provided and billed for by a provider have been explicitly excluded from this research, as they are more challenging to prove, are often associated with simple inefficiencies and

incompatibilities in the healthcare system, and can call into question the subjective medical opinion of providers which can be hard to substantiate. While waste is a significant problem, it is less tractable and comparable to other industries than fraud and abuse. In this review, the CMS definitions for fraud and abuse are adopted:

- **Fraud**: Purposely billing for services that were never given or billing for a service that has a higher reimbursement than the service produced
- **Abuse**: Payment for items or services billed by mistake by providers but should not be paid for by Medicaid

4.3.2 Fraud Strategies

Sparrow (Sparrow, 2000) describes two polar extremes in a fraud strategy spectrum: the "hit-and-run" and the "steal a little, all the time" schemes. The hit-and-run is a short-term strategy to bill for and acquire large amounts of money quickly and disappear before anyone realizes what happens. At the opposite extreme lies the criminal who steals a little all the time. Legitimate healthcare providers who provide genuine services use their bulk of legitimate claims to hide incremental stealing.

Medicaid	Telecommunications	Credit Card
Hit and run	Subscription fraud	Application fraud
Steal a little all the time	Superimposed fraud	Behavioral fraud

Table 2 - Types of Fraud Across Industries

Similarities exist in the telecommunications industry, with subscription fraud (false identification and no intention to pay) and superimposed fraud (slow and hidden) (Cahill et al., 2002). Parallels in the credit card industry include application and behavioral fraud (Bolton & Hand, 2002) (see Table 2). A significant difference between the aforementioned "hit and run" and "steal a little all the time" schemes is the degree to which they are self-revealing (Sparrow, 2000). The "hit and run" parallels in the telecommunications and credit card industry are self-revealing because customers, not insurance companies or governments, are losing money rapidly, and both see and pay the bill. The "steal a little all the time" comparators are likely more applicable, as customers may not notice small bill changes. Table 3 highlights and categorizes some known Medicaid fraud schemes (Hast, 2000).

Fraud Scheme	Short Explanation	Type
Identity Theft	Stealing identification information from providers or beneficiaries and using that information to submit fraudulent bills to Medicaid.	Fraud
Fictitious Practitioners	Enrolling and submitting bills to Medicaid on behalf of fictitious practitioners	Fraud
Phantom Billing	Submitting claims for services not provided.	Fraud
Duplicate Billing	Submitting similar claims more than once.	Fraud/ Abuse
Bill Padding	Submitting claims for unneeded ancillary services to Medicaid.	Fraud/ Abuse
Upcoding	Billing for a service with a higher reimbursement rate than the service provided.	Fraud/ Abuse
Unbundling	Submitting several claims for various services that should only be billed as one master claim that includes ancillary services.	Fraud/ Abuse

Table 3 - Medicaid Fraud Schemes (partially derived from Hast(Hast, 2000))

4.4 Overview of Relevant Fraud Detection Techniques and Papers

Table 4 shows a typology of fraud detection techniques discovered in the literature review. This typology is used in Table 5 to classify the papers.

Type	Method	Explanation
A	Supervised Classification Techniques	Use training sets with prior information on class membership to learn classification patterns
A1	Linear Discrimination	Regression-based on a logistic curve
A2	Support Vector Machines	A kernel method that selects a small number of critical boundary instances (support vectors) to construct a separating hyperplane(Sudjianto et al., 2010)
A3	Neural Networks	A set of interconnected nodes that imitate the functioning of a brain(Kou et al., 2005)
A4	Decision Tree Learning	Methods for building a decision tree for classification
B	Unsupervised Data Mining Techniques	Do not assume prior class labels of legitimate or fraudulent behavior
B1	Anomaly Detection	Tries to detect outliers that are inconsistent with the remainder of that data set(Grubbs, 1969; Pincus, 1995)
B2	Cluster Analysis	Divide objects into groups (clusters), with objects in a group being similar to one another but dissimilar to the objects in other groups(Ngai et al., 2011)
B3	Peer Group Analysis	Clusters of similar observations (peer groups) are identified and clustered; subsequently, the individual behavior is compared to the cluster's behavior (Bolton & Hand, 2001)
C	Statistical Methods	Statistical methods are more model- and theory-based than Data Mining methods
C1	Visualization	Allowing users to view the complex patterns or relationships uncovered in the data mining process(Turban et al., 2011)
C2	Profiling	Process of modeling the characteristic aspects of the user (Fawcett & Provost, 1997)
C3	Benford's Law	The distribution of the first-digit number of many natural phenomena like the size of companies, telephone lengths, and invoice amounts will have a characteristic non-uniform distribution. (Hill 1995; Nigrini 1999)
D	Rule Based	Model based on the experience of experts (Bolton et al., 2002b)
D1	Online Analytical Processing (OLAP)	Dynamic ad-hoc multidimensional analysis (Codd et al., 1993)
D2	SQL Queries	Queries designed by domain experts

Table 4 - Overview of Fraud Detection Techniques

The structured literature review about fraud detection systems resulted in an overview of applied fraud detection techniques by industry (Table 5).

	Paper	Objective	Method	Results/Findings
Credit Card	**Unsupervised Profiling Methods for fraud detection** (Bolton et al., 1999)	Apply unsupervised techniques when labeled data is unavailable.	B3 C2	Both analysis and visualization can detect anomalies and detect changes in spending trends.
Credit Card	**Neural Fraud Detection in Credit Card Operations** (Dorronsoro et al., 1997)	To present an applied online fraud detection system (Minerva).	A3	Positive result: It detects 40% of all fraudulent transactions and can be used as a basis for other models.
Credit Card	**Data mining for credit card fraud: a comparative study** (Bhattacharyya et al., 2011)	To evaluate random forests and support vector machines.	A2 A4	Random forest-based methods achieve good overall performances.
Finance	**Statistical Methods for fighting Financial Crimes**(Sudjianto et al., 2010)	To provide a survey of statistical techniques and data mining.	A B1 B2 C2	To provide an overview of financial fraud.
Finance	**The application of data mining techniques in financial fraud detection** (Ngai et al., 2011)	To review data mining techniques to discover financial fraud.	A B1 B2 C1	A review of 49 articles to categorize financial fraud and an overview of applicable data mining techniques.
General	**Survey of Fraud Detection Techniques** (Kou et al., 2005)	To provide a comprehensive review of different fraud detection techniques.	A3 B1 C1 D	Neural networks are an essential tool; however, they are challenging to implement due to a lack of data. Profiling to detect fraud from call patterns is effective.
General	**Statistical Fraud Detection: A Review** (Bolton & Hand, 2002)	To describe the statistical tools available in the different areas.	A B1 C1 C2 D	The speed of detection is essential and should be measured. Statistical approach effectiveness depends on the type of problem.
General	**A Comprehensive Survey of Data Mining-based Fraud Detection Research** (Phua et al., 2010)	To define existing challenges in the fraud detection domain for large data sets.	A B2 B3 C2	Overview of Supervised, semi-supervised, and unsupervised techniques.
General	**A Taxonomy of Frauds and Fraud Detection Techniques** (Laleh & Azgomi, 2009)	A taxonomy of (new) frauds and fraud detection techniques.	High-level overview of A &	The result is an overview of several types of fraud and fraud detection

	Paper	Objective	Method	Results/Findings
			B	techniques on a high level, including (un)supervised and semi-supervised techniques.
Healthcare	**Holistic Approach to Fraud Management in Health Insurance** (Furlan & Bajec, 2008)	Overview of fraud management: Detection is just one step in the process	A B C	Fraud management is just as important as fraud detection. A case study supports their prepositions.
Healthcare	**EFD: A Hybrid Knowledge/Statistical-based System for the Detection of Fraud** (Major & Riedinger, 1992)	Electronic fraud detection.	C D	True positive rates are approximately 50% with the applied set of heuristics.
Telecom	**Fraud Detection in Telecommunications: History and Lessons Learned** (Becker et al., 2010)	To discuss major fraud schemes and fraud detection techniques used to address them.	C1 C2 D	Use simple, understandable models with visualization and human involvement.
Telecom	**Novel Techniques for Fraud Detection in Mobile Telecommunications Networks** (Moreau et al., 1996)	To explore detecting fraudulent behavior based on absolute and differential behavior.	A C2 D	Obtaining significant fraudulent data and labeling it as such is a considerable effort and often a problem.
Telecom	**Adaptive Fraud detection** (Fawcett & Provost, 1997)	To describe a design of user profiling methods.	C2 D	Fraud detection systems must be adaptive. People must determine (trial-and-error) how to profile and which rules are effective.
Telecom	**Establishing Fraud Detection Patterns Based on Signatures** (Ferreira et al., 2006)	To detect inappropriate behaviors within a useful period of time.	B1 C2	The anomaly detection with the signature as a basis supports telecom fraud detection.

Table 5 - Overview of Relevant Fraud Detection Papers

Some papers discuss fraud detection in the healthcare industry. Major and Riedinger (1992) addressed this topic 19 years ago, and, more recently, Furlan and Bajec (2008) touched on this topic from a holistic point of view,

highlighting the importance of fraud detection and the broader scope of fraud management.

4.5 Lessons Learned for Medicaid

The foundations of fraud detection across the various industries studied are underpinned by electronic fraud detection mechanisms that flag suspicious transactions for further review. These sophisticated systems must evaluate mass amounts of information and match simple and complex patterns. Systems must be paired with humans knowledgeable of appropriate and inappropriate practices to interpret the data and judge if a transaction should be flagged as fraudulent (Hand, 2010). While Medicaid possesses its structural complexities, a great deal of progress can be made with the help of electronic and human data-driven fraud detection techniques.

Stakeholder feedback, or the lack thereof, makes automated electronic mechanisms even more important in government healthcare fraud control. Ideally, stakeholders should be incentivized, willing, and able to offer information indicating fraudulent behaviors. In the credit card and telecommunications industries, customers immediately report fraud, as it is in their personal financial best interests to do so. With health insurance, even if a beneficiary notices a mistake on an EOB, they are inclined to think that someone else is paying, so why worry about it (Sparrow, 2000)? Thus, little feedback is provided from beneficiaries on the legitimacy of claims to state Medicaid agencies.

The credit card and telecommunications industries possess real-time data, quickly resolve reported cases of fraud, and, as such, maintain high-quality databases of labeled data that can be used for supervised learning. Medicaid data is dispersed and unlabeled, and there are no signals that this will change soon. Multiple stakeholders at the federal and local levels, misaligned incentives, and fragmented responsibility hamper the process of labeling and sharing data. Thus, supervised learning techniques are severely restricted.

Improvement is needed in the feedback loop of prosecutions and post-payment adjustment to label the source claims data with high-certainty adjudications that could be leveraged for supervised learning. This should

be a joint effort of the federal government, states, and the commercial health insurance industry to improve the data supply and enable the co-development and sharing of fraud models that could apply across the healthcare industry.

It should be noted that the insurance industry has much tighter controls around the providers of services, be they healthcare practitioners, auto body shops, or home construction contractors. Providers are modeled and compared, and providers with costs above an acceptable range are excluded from participation and reimbursement under the insurance policy. In contrast, all providers are welcome to participate in Medicaid programs and can only be excluded based on fraudulent activities.

Supervised classification models are particularly appropriate for healthcare fraud, as they can be trained and adjusted to detect sophisticated and evolving fraud schemes. Supervised classification techniques like neural networks, support vector machines, and random forests form the basis for sophisticated and effective fraud detection in the credit card industry. The drawback to these techniques is that new fraud schemes are not immediately detectable due to the lag of discovering and labeling new fraud in training data. Unsupervised methods such as profiling and anomaly detection are applied in the telecommunications industry to complement supervised learning. In the telecommunications industry, high-quality data is available to construct accurate profiles. Computer security and intrusion detection utilize supervised techniques to discover and detect known patterns and anomaly detection to detect new, unique intrusions. Unfortunately, with healthcare's more diverse set of outcomes and patterns, applying unsupervised techniques suffers from a high false-alarm rate because outliers do not necessarily imply fraudulent or abusive behaviors but rather the diversity of patterns of care and practitioner prerogatives.

All these industries have an essential advantage over Medicaid: they all possess accurate, real-time, and labeled data. Furthermore, these industries are supported by stakeholders who report unusual events and behavior because these events affect them directly. These commercial industries and their customers do not want to lose profit; therefore, they are willing to allocate the necessary resources to remove fraud from the

system. These industries and companies realize that fraud detection is vital to doing and staying in business. Medicaid's prioritization of timely payments over accurate, fraud-free payments disadvantaged the program from the start. Additionally, the number of stakeholders involved and the fragmented responsibilities further complicate fraud control. With today's technologies and the cooperation of those with knowledge of ground truths, much progress can be made in fighting Medicaid fraud using supervised and unsupervised techniques guided by subject matter and data experts.

Modern modeling, scoring, and business intelligence tools can be used to apply some of these techniques. For example, practical anomaly detection and peer group analysis can be performed and automated when combining claims history with geographically and socioeconomically adjusted provider models. Using dashboards and visualization tools, problematic providers quickly stand out and raise flags for targeting. Business intelligence tools can serve as an essential monitoring instrument for payment trends by various dimensions that could signal fraud. For example, a localized criminal enterprise may be at play if the Medicaid payment profile across provider types suddenly diverges from historical norms and recent national trends for a specific geographic area. Developing these models with appropriate environmental variables is challenging, but today's business intelligence, modeling, and scoring tools make their real-world application practical and achievable.

4.6 Conclusions

Given that Medicaid is the payer of last resort and receives little feedback from the actual beneficiary of paid healthcare services, the dependence on electronic fraud detection is significantly greater than in similar studied industries. As learned from the credit card industry, telecommunications, and computer security, fraud detection using supervised classification can be highly effective. However, the base requirement for this approach (labeled data) is currently unavailable across the Medicaid program. The benefits of supervised learning techniques should be weighed against the costs of streamlining data acquisition and closing the feedback loop from adjudicated claims to labeled claims data. Given the high rate of fraud estimates across Medicaid and the program's overall expenditures, it is

unfathomable that these IT and business process problems could not be overcome for orders of magnitude less investment than the dollars lost to fraudulent behavior in the program.

The analysis showed that supervised techniques are necessary for an effective fraud detection system. Furthermore, the extensive application of classification techniques in various domains proves their effectiveness and utility in contributing to fraud detection. However, no one technique, supervised or unsupervised, will address all fraud strategies and schemes. A fraud detection system consisting of multiple techniques, with a flexible, modular approach capable of adapting to the continuous changes in the fraud detection field, must be employed to combat fraud and abuse effectively.

Over time and with increasing levels of sophistication in fraud control systems, empirical testing must be performed to evaluate their efficacy. Evaluation criteria should include the detection rate, effort, interpretability, and return on investment. The corresponding costs of developing a fraud detection system should be offset and weighed against the resulting benefits of the fraud detection system. What are the strengths and weaknesses of the system, and how can its performance be enhanced? Applying data collection and fraud detection techniques in practice through a state-centric pilot program would help determine the effectiveness of various approaches.

A significant limitation of this study is its theoretical approach. A systematic literature study has been conducted to provide an overview of the current problematic situation in Medicaid and what electronic fraud detection techniques exist in related fraud detection domains. Published fraud frameworks are limited, as fraudsters would benefit from easy access to the information and would undoubtedly attempt to use that sensitive information to enhance their fraud techniques. While not an ideal investigation, the literature review provides a proper first impression and overview of the existing fraud schemes and detection techniques currently applied across similar industries.

Future research should be undertaken to evaluate the current methodologies and tools employed by states and CMS to detect and

prevent fraud and assess the potential impact of the methods discussed in this paper. In addition, while not a technology problem, an in-depth assessment should evaluate the effects of Medicaid policy changes, such as increasing Medicaid provider enrollment standards, delaying payment to allow for more claim review time, or providing incentives to report fraudulent activity found on EOBs.

The high number of stakeholders, 50 states with unique legislation and eligibility rules, and the sheer magnitude of the program complicate Medicaid fraud control efforts. As Sparrow (2000) explains, fraud should be measured appropriately to create a realistic impression of the current situation and estimate the amount of fraud and abuse in the system. The Thompson Reuters estimation (Kelley, 2009) of $600 to $850 billion lost to fraud, waste, and abuse annually is only an estimate. Without significant, periodic audits of randomly sampled claims across the Medicaid system, it is impossible to accurately estimate the level of fraud, waste, and abuse in the system and its change over time. Although fraud will never be eradicated, it can be better managed with systematic improvements in data collection, applied detection and prevention tools, better incentive structures, and enforcement actions.

4.7 Recent Updates to Literature Review

Recent progress has increased publications in the healthcare fraud detection space; however, due to the healthcare domain's confidentiality and privacy aspects, published work remains more limited than is prevalent in commercial insurance and accounting domains. Notable recent publications are classified and described below, including a discussion of potential applications to Medicaid fraud detection.

4.7.1 Healthcare

4.7.1.1 Blockchain

Saveetha and Maragatham (2022), W. Liu (2019), Gera (2020), Saldamli (2020), Ismail and Zeadally (2021), and Vyas (2022) discuss incorporating blockchain-based distributed ledgers in the claims processing process to increase transparency and improve data veracity.

Kapadiya (2022) extends the blockchain for claims approach to smart contracts, proposing additional patient telemetry streaming from wearable

devices to health insurers to improve fraud detection modeling in exchange for compensation from insurers via smart contracts.

Lakhan (2022) proposes using blockchain for healthcare Internet of Things (IoT) data storage and analysis for fraudulent data, exploring a layered approach to training and model application, beginning closer to the data source to reduce computational and energy costs. The computational performance characteristics of this approach were evaluated using healthcare provider claims to predict provider fraudulence based on training set data.

Blockchain offers unique approaches that could enhance the veracity of claims, provider, and other data sets that can often be problematic in fraud detection. Utilizing this technology would require a significant investment and shift in provider and beneficiary enrollment and management systems. This would be challenging for a single insurer. With Medicaid, this would require a retrofit and replanning of every state system or the buy-in of every state to use a single federal system. This is politically and practically fraught, with the realization of theoretical benefits a long way out.

4.7.1.2 Data Modeling

Matloob and Khan (2019) apply modeling to patients, providers (doctors, hospitals, and pharmacies), and services, using data from operational healthcare systems from various departments (instead of claims data) and apply clustering methodologies and outlier detection. This more detailed signal data from systems closer to the encounter identifies anomalies within and across the modeled entities.

Fursov (2022) demonstrates an approach to transform relational claims data into a graph, embedding object descriptions in vectors with the same dimensionality as the graph nodes. This enables Neural Network approaches for analysis that outperform traditional machine learning approaches.

J. M. Johnson and Khoshgoftaar (2020) present a graph vector development and evaluation method using Healthcare Common Procedure Coding System (HCPCS) codes embedded in claims. Word2Vec models derive semantic relationships between HCPCS codes, providing better context than traditional, analysis context than traditional one-hot vector

development with claims data alone by correlating like and related procedures. (Haque and Tozal, 2022) demonstrate a modeling approach to translate diagnosis and HCPCS codes into Mixtures of Clinical Codes (MCC), providing improved context to claim validity. These approaches to improving the information gained from simple codes are promising to enhance downstream clustering and outlier identification.

Settipalli and Gangadharan (2023) propose a graph model for classifying and comparing providers' behavior, incorporating provider reference data, such as specialty and credential, and claims information, including place of service, zip code, and HCPCS codes.

W. Zhang (2022) demonstrates a graph modeling and analysis approach to uncovering multiparty prescription fraud across pharmacies, providers, and patients.

Zhao (2019) proposes a methodology for developing and analyzing a "Dynamic Heterogeneous Information Network" graph, modeling the relationships between patients, providers, hospitals, conditions, and treatments. This promising approach could potentially be enhanced by J. M. Johnson & Khoshgoftaar's (2020) HCPCS2Vec methods and additional source data that improve the veracity of graph node data.

J. M. Johnson and Khoshgoftaar (2022) demonstrate the usefulness of CMS's Medicare Part B "Summary by Provider" (SbP) and "Summary by Provider and Service" (SbPS) data sets in providing additional feature context to provider claim behavior.

Matloob (2020) demonstrates the usefulness of using time-series claims data to develop sequences of care that represent normal and abnormal behavior.

Settipalli and Gangadharan (2023) propose a graph model for classifying and comparing providers' behavior, incorporating provider reference data, such as specialty and credential, and claims information, including place of service, zip code, and HCPCS codes.

Recent data modeling research – specifically graph modeling and analysis – offers significant benefits to understanding the networks of actors and interactions that have been hard to analyze with traditional techniques. As

discussed in subsequent chapters, this will become a significant driver for modern fraud detection in complex, multi-stakeholder systems.

4.7.1.3 General Data Analytics

Nazir (2020) reviews the current work of analytics in big data across the healthcare space. This is not limited to fraud detection but provides a broad view of activities.

Thomas and Judith (2020) present an outlier detection method using a one-class support vector machine (SVM) alongside an autoencoder. Applied to a limited dataset of cancer data, the approach fared well in discriminating outliers vs. employing only the SVM or autoencoder alone. Applied to healthcare fraud detection, hybrid risk evaluation methods are similarly needed to improve the discernment of outliers and reduce false positives.

Jain and V (2021) provide a review of data mining algorithms used across various fields in healthcare.

Nazir (2019) provides a literature review covering the use of big data in the cardiology domain. Diving deep into a specific domain within healthcare, such as cardiology, offers guidance in developing signals to monitor the domain to improve observability and the usefulness of the data in fraud detection.

Harerimana (2018) surveys recent analytics technologies employed in healthcare intended as a “do-it-yourself” guide for health analytics application developers.

Kumar and Singh (2019) highlight current big data technologies applicable across healthcare, including HDFS, MapReduce, and many interesting Apache projects. Pramanik (2022) highlights the challenges of using big data in healthcare and surveys current “tools and platforms, architectures, and commercial infrastructures for healthcare big data.”

Bahri (2019) discusses current big data technologies and evaluates how they could impact various healthcare contexts, including “Healthcare monitoring, Healthcare Prediction, Recommendation systems, Healthcare Knowledge systems, and Healthcare Management Systems.”

Alharbe (2022) conducts experiments on outlier detection, comparing statistics-based, traditional k-nearest neighbors (KNN) and a proposed improved KNN-based approach. It offers a KNN approach that enhances accuracy and reduces time complexity.

Purandhar (2022) proposes a generative adversarial network approach to classification, which compares well to support vector machine, decision tree, and random forest algorithms on two healthcare datasets in cardiology and lung cancer.

M. Chen (2017) proposes a convolutional neural network approach for predicting cerebral infarction tested using both structured and unstructured Chinese hospital data from 2013-2015.

Boddy (2019) proposes a density-based outlier detection approach to detecting improper access to patient records within an electronic health records system. This information security approach could apply similarly to fraud detection with increased stakeholder and transaction telemetry.

These references offer examples of applying analytic methods in the broader healthcare field.

4.7.1.4 Fraud Detection Approaches

Sumalatha and Prabha (2019) demonstrate a logistic regression and a multi-criteria decision analysis (MCDA) process that improved healthcare fraud detection for an Indian insurer.

Ekin (2018) provides an overview of statistical methods and areas of development in healthcare fraud detection research.

Yao (2021) proposes and demonstrates the efficacy of an improved bootstrap aggregation (Bagging) algorithm in detecting Medicare fraud. Bagging (bootstrap aggregation) algorithm to detect Medicare fraud. The weighted threshold method, WTBagging, improves on a traditional Bagging model, basing results on a weighted ensemble approach.

Ai (2022) provides a recent systematic PRISMA-based literature review of fraud detection methods in healthcare from 2001 to 2016, including methods published previously and included in this thesis.

Duman and Sağıroğlu (2017) review healthcare fraud detection literature, focusing on analysis techniques, data sources, and data characteristics. Unsupervised techniques were the most frequently cited, as reliable labeled data is challenging to obtain.

Liang (2019) presents an approach to evaluating potential collusion in healthcare network participants based on device utilization in China. This approach could have parallel applications in technical interactions with providers and patients with healthcare systems, as well as modeling medical billers akin to the "device" concept. Unfortunately, much of this system and "hidden" participant information is currently unavailable to claims processing and would need to be studied to evaluate collection methodologies and interactions with privacy requirements.

Luan (2019) demonstrates the effectiveness of modeling relationships between doctors and drugs prescribed as a clustering and outlier detection mechanism. This paper confirms and references the approach from the Medicaid dental domain work from Chapter 6 in a different medical domain.

Akbar (2020) evaluates the analytics approach in healthcare fraud detection and demonstrates the usefulness of XGBoost in detecting fraudulent claims in a Medicare dataset.

Hancock and Khoshgoftaar (2022) demonstrate the positive impact of increasing the tree depth of XGBoost and Random Forest algorithms on Medicare claims data. This follows from the high cardinality of claims data – significant overloads of data fields are used to distill complex medical situations into standard claims processed by insurers. Increasing tree depth (with abundant training data) begins to unravel the permutations of actions that represent repeated activities across medical sub-domains without overfitting.

Hancock and Khoshgoftaar (2020a) demonstrate the usefulness of CatBoost in classification for healthcare fraud detection. Further, they (2020b) show the significant impact of adding features from reference data to bring context to CatBoost and XGBoost classification claims.

Castaneda (2019) evaluates Maxout neural network approaches to classification in healthcare fraud detection, comparing the effectiveness of Maxout variants.

Sadiq (2017) demonstrates an anomaly detection approach based on the Patient Rule Induction Method (PRIM) to flag physicians behaving abnormally. Results showed marked improvement in identifying risky providers more likely to commit fraud.

R. Bauder (2017) surveys recent literature on algorithmic methods to analyze or detect healthcare claims upcoding.

Anbarasi and Dhivya (2017) highlight the challenges of combining retrospective and proactive analysis. The proposed approach implements graph data modeling in a "policy verification module" preprocessing step and an outlier detection module that operates on the graph to clean further and filter the data, compute metrics, compare actors by metrics, and flag outliers. This continuous process updates the risk scoring of providers in the methodology.

J. Zhang (2022) demonstrates a Graph Neural Network (GNN) based methodology for temporal and multi-modal data that evaluates across heterogeneous graph nodes and neighbors. Similarly, Yoo (2022) and Wang (2022) demonstrate the efficacy of a graph sample and aggregate (GraphSAGE) based GNN in Medicare fraud detection. These approaches offer promise when applied to complex graph data sets representing healthcare relationships and transactions.

Sun and Li (2019) highlight a graph-based approach to clustering inpatient episodes of care and patients by demographics and then evaluating for similarities of similar patients to claimed patterns of care. Graphs can represent patterns of care much more directly and performantly than evaluating flat relational data, improving the efficacy of overall risk modeling.

Zhu (2011) demonstrates a nonnegative matrix factorization approach to clustering for healthcare fraud detection. It remains to be seen how this technique compares with alternate clustering approaches, and it adds

practical challenge to increasing data dimensionality and relationship context from additional data sources over time.

Vyas and Serasiya (2022) highlight several approaches being evaluated for healthcare fraud detection, focusing on India and blockchain technology.

Alam (2022) proposes supervised techniques for fraud detection and homomorphic encryption that could provide enhanced security and privacy preservation. Given the data correlation across sources needed, there is potential for separating data engineering and data science activities. However, the small scale of fraud prevention teams vs. the added benefit of this approach would be hard to justify in current operational models.

Kumaraswamy, Markey, and Ekin (2022) provide a recent review of fraud detection methods in healthcare, highlighting gaps in the applicability of current published literature to real-world implementation. The findings in this paper align with the experiences highlighted in this thesis working within the US Medicaid system.

R. A. Bauder (2019) evaluates the effectiveness of separate training and test data sets, as characterized by Bengio and Grandvalet (2003), vs. cross-validation, as proposed by Gupta (2017). In analyzing Medicare claims data for fraud, separate test and training data sets were shown to improve accuracy. However, cross-validation was effective when different data sets were not feasible.

Settipalli (2022) presents the concept of "Drift Analysis in Decomposed Healthcare Claims (DADHC)" to evaluate and compensate for sudden or gradual shifts in a provider's claims behavior that seasonality, pandemics, or shifts in standards of care could explain. The study evaluates various approaches for windowing and proposes a topological clustering approach. Patterns of care change over time, and clustering models must consider this to minimize false positives.

Rawte & Anuradha (2015) presents a hybrid approach combining supervised (SVM classification) and unsupervised (Evolving Clustering Method, ECM) to provide responsiveness and adaptability to incoming data. Specifically, ECM continuously adapts clusters that could represent new disease modalities based on incoming data. In contrast, SVM uses this

cluster affinity and other claim features, such as date, to classify appropriate claims as fraudulent, such as duplicate billings. This layered approach demonstrates how ongoing analysis can develop and maintain features that add context to the claims analysis.

Rayan (2019) describes a hybrid framework for healthcare fraud detection, including a rules engine, supervised learning through decision trees and averaged perceptron, and unsupervised methods, such as clustering, outlier analysis, and k-means. The system provides auditors with a prioritized queue of claims with comments regarding why the claims are likely to be fraudulent.

Building on the work presented in Chapter 6, Kumaraswamy, Markey, and Barner (2022) evaluate feature selection in pharmacy claims, analyzing 176 facets and distilling 15 features that represent 85% of claim variance. Addressing known actor relationships in various potential fraud schemes, "A set of features were engineered following a logical inference of interactions between potential fraudulent actors." The work provides an analytical framework for converting prescription claims to features to fraud indicators.

Kareem (2017) demonstrates the usefulness of clustering and association rule mining in detecting fraudulent transactions in Malaysian healthcare data. Verma (2017) also showed positive results from clustering and outlier analysis, evaluating period of care and disease-based patterns of care as critical discriminators.

S.K. and Ilango (2020) propose and demonstrate a feed-forward neural network classifier with a genetic algorithm optimization working atop CMS Medicare claims data pre-processed with PCA for feature selection and reduction.

Mehraby (2022) evaluates the claims analysis and target selection process for an Iranian health insurer using a dataset of 100k claims and evaluates the assessment process over a year. It offers insight into approaches that could improve the targeting and assessment process, including the need for assessors to understand the methodology for the cases they are assigned clearly. It proposes clustering and rules association mining with visualization provided to assessors that can be clearly understood.

Gao (2018) proposes an approach for fraud detection in mobile healthcare claims combining results from SSIsomap pattern matching and SimLOF outlier detection using Dempster's Rule of Combination to provide a fraudulence probability used for decision support. The methodology was tested with 40M claims across 40k patients from the Dareway Medical Insurance System in Zibo City, China.

S. Chen and Gangopadhyay (2013) apply spectral analysis to a two-mode network to detect communities and potential collusion between primary care providers and specialists. This approach could be extended to additional actors as those relationships are identified and added to the graph.

Zhou and Zhang (2020) propose erring and Local Outlier Factor (LOF), evaluating effectiveness using 390k records from a Chinese healthcare insurer. The risk scoring method developed now supports auditor decision support for the company.

Matloob (2022) applies sequence mining at a specialty, or sub-domain, level to determine normal and anomalous patient service sequences. These rules were informed by data but guided by medical experts in determining "frequent medical behaviors." Abnormal sequences can add to risk scoring or trigger audit activities.

Sun and Yan (2019) propose methodologies for person similarity calculation and abnormal group mining, resulting in normal vs. suspicious group scoring. The model was evaluated using 40M records spanning 10k patients and improved on L-SVM classification, DILOF anomaly detection, BP-Growth pattern mining, and Abnormal Growth methods.

Significant progress has been made in published research in the field over the past decade. Many data science techniques are successfully leveraged to tackle healthcare fraud globally. I expect the field to continue to mature. I hope to see an open-source library of ML models, data models, and data management techniques emerge over time, making the shared societal problem of healthcare fraud one we can all combat.

4.7.2 Other Industries

4.7.2.1 Analytic Approaches

Jing (2019) proposes a graph-based credit card fraud detection framework using GraphSAGE on node classification. This approach offers promise in healthcare fraud as additional reference datasets and probabilistic relationships discerned from claims patterns are added to provide context to claims data.

Dhieb (2020) develops a framework for applying machine learning models to blockchain-resident data. Specifically, XGBoost and VFDT algorithms were evaluated for classification and risk scoring for auto insurance claims and customers and implemented for a commercial insurer.

Omair and Alturki (2020) provide a systematic literature review of fraud detection in business process-based fraud, covering metrics and analysis approaches relevant to the field. The approaches, complex process environments, and limited observability constraints offer significant similarities to healthcare fraud detection.

Meng (2022) demonstrates the usefulness of a user behavior attribute matrix and adjacency matrix, employing CUR matrix decomposition to detect abnormal behaviors on the network. The approach was successfully tested against the public MAWI dataset and data collected from CERNET.

Ashtiani and Raahemi (2022) provide a Kitchenham-based systematic literature review of techniques used for fraud detection in financial statements.

Ali (2022) offers a recent literature review of financial fraud detection based on machine learning. Analytical techniques, common types of fraud, and methods for evaluating results are included.

These novel approaches, applied in other industries, offer promise in healthcare fraud detection.

4.7.2.1 Business Use of Analytics

In qualitative research evaluating the impacts of adding big data analysis to audit brainstorming sessions, Marei (2022) highlighted the positive effects of surfacing risk indicators to auditors. “Auditors… highlighted that the

emerging Big Data is assessed in terms of its effect on audit evidence's sufficiency, competence, and reliability. The evidence usually derived from the external context is more probabilistic and must be weighed considering information's characteristics." The work highlighted the importance of context and lineage in providing big data inputs to the audit process.

5

Chapter 5: A Multidimensional Data Model and Analysis Techniques for Fraud Detection

Adapted from:

Dallas Thornton, Roland M. Mueller, Paulus Schoutsen, Jos van Hillegersberg: Predicting Healthcare Fraud in Medicaid: A Multidimensional Data Model and Analysis Techniques for Fraud Detection, Procedia Technology, Volume 9 (2013) Pages 1252–1264.

Chapter 5: A Multidimensional Data Model and Analysis Techniques for Fraud Detection

5.1 Introduction

In this chapter, Hevner (2004) is applied to help develop a framework for fraud detection in Medicaid that provides specific data models and techniques that identify the most prevalent fraud schemes and should help identify the unknown unknowns. Section 5.2 discusses the environment, including payers, providers, and patients. Section 5.3 covers the knowledge base, represented by fraud detection literature and the state of the industry. Based on this analysis, section 5.4 proposes a multidimensional schema based on Medicaid data and describes a set of multidimensional models and techniques to detect fraud in large sets of claim transactions. Section 5.5 evaluates these artifacts through functional testing against known fraud schemes. Healthcare fraud control must address the unknown unknowns. This chapter offers a set of multidimensional data models and analysis techniques that can detect the most prevalent known fraud types and should assist in detecting the unknown unknowns.

5.2 Environment

The following definition of fraud from the US Department of Health and Human Services (Department of Health and Human Services, 1998) will be used for the purposes of this chapter: “Fraud is the intentional deception or misrepresentation that an individual knows to be false or does not believe to be true and makes, knowing that the deception could result in some unauthorized benefit to himself/herself or some other person.” Three main parties commit fraud within the healthcare system: healthcare providers, beneficiaries (patients), and insurance carriers. Providers are the initiating actors for billing insurers and, as such, quickly become the nexus for fraud schemes. When a provider participates in Medicaid, the provider agrees to the reimbursement rates set by the state and submits claims for payment directly to the state or managed care entity. If the provider is not participating in Medicaid, the provider sends the patient the bill, which they pay before requesting Medicaid reimbursement. The agency or insurer processes the claim and sends an explanation of benefits to the patient that describes the services paid for along with their codes and costs.

States operate claims processing systems that perform various prepayment checks and edits to inspect the claim's legitimacy. Edits and audits verify information with honest providers in mind, but they are not designed to detect fraud schemes of any depth (Sparrow, 2000). These systems cannot verify whether the service was provided as claimed, the diagnosis is correct, or whether the patient is even aware of the services.

5.3 Knowledge Base

5.3.1 Classifying Fraud

Sparrow (2000) describes two types of fraud: "hit-and-run" and "steal a little, all the time." "Hit-and-run" perpetrators simply submit fraudulent claims, receive payment, and disappear. "Steal a little, all the time" perpetrators work to ensure fraud goes unnoticed and bill fraudulently over a long period. The provider may hide false claims within large batches of valid claims and, when caught, will claim it as an error, repay the money, and continue the behavior. The FBI (Federal Bureau of Investigation, 2009) highlights and categorizes some of the most prevalent known Medicaid fraud schemes:

- Phantom Billing – Submitting claims for services not provided.
- Duplicate Billing – Submitting similar claims more than once.
- Bill Padding – Submitting claims for unneeded ancillary services to Medicaid.
- Upcoding – Billing for a service with a higher reimbursement rate than the service provided.
- Unbundling – Submitting several claims for services that should only be billed as one service.
- Excessive or Unnecessary Services – Provides medically excessive or unnecessary services to a patient.
- Kickbacks – A kickback is a form of negotiated bribery in which a commission is paid to the bribe-taker (provider or patient) as a quid pro quo for services rendered (Albrecht, 2012).

Sparrow (2000) proposes that for effective fraud detection, one has to look at the data beyond the transaction level, defining seven levels of healthcare fraud control (see Table 6).

		Level Focus
Level 1	Single Claim, or Transaction	The claim itself, the related provider, and the patient.
Level 2	Patient / Provider	One patient, one provider, and all their claims.
Level 3	a. Patient	One patient, all its claims, and related providers.
	b. Provider	One provider, all its claims, and related patients.
Level 4	a. Insurer Policy / Provider	Patients that are covered by the same insurance policy and are targeted by one provider.
	b. Patient / Provider Group	One patient being targeted by multiple providers within a practice.
Level 5	Insurer Policy / Provider Group	Patients with the same policy being targeted by multiple providers within a practice.
Level 6	a. Defined Patient Group	Groups of patients being targeted by providers. (i.e., patients living in the same location)
	b. Provider Group	Groups of providers targeting their patients. Groups can be providers within the same practice, clinics, hospitals, or other arrangements.
Level 7	Multiparty, Criminal Conspiracies	Multiparty conspiracies that could involve many relationships.

Table 6 - Levels of Healthcare Fraud Control (Adapted from Sparrow (2000))

Each higher level involves larger fraud schemes with more people involved and an increased difficulty of being detected. According to Sparrow (2000), most of the industry's detection toolkit focuses on levels 1 and 3. Before payment, the transaction (level 1) and patient level (level 3a) may be evaluated. For example, are there claims for multiple childbirths within nine months? Post-payment analysis may focus on the provider level (level 3b). For example, is a doctor billing more hours of office visits than possible?

5.3.2 Context in Fraud Detection Literature

The literature about healthcare fraud can be divided into three categories. The first category provides an overview of the field. It focuses on what kind of statistical methods can be used. For example, Travaille (2011) created an overview of statistical methods used by fraud detection within other industries and how they can be applied within the healthcare industry. Li (2008) surveyed healthcare industry methods and found combinations of unsupervised and supervised methods used together with profiling. The second category provides results on actual applications of the methods to find their usefulness in detecting fraud. For example, Copeland (2012)

discussed unsupervised methods to find Medicaid fraud within Nevada. Yang and Hwang (2006) looked at using the order in which services are performed for fraud detection. This category helps in choosing a method for fraud detection by comparing the results of individual methods.

The third category is focused on general methods and models to improve fraud detection. For example, Morris (2009) describes five critical components of changing the health system to better battle fraud. Major and Riedinger (2002) describe a workflow and system to set up fraud detection departments with results of its use in the real world. Similar work was done by Ortega (2006), who introduced a data mining-based system that decreased the time it took to detect fraud by 76% from an average of 8.6 months to 2 months. Because Major, Riedinger, and Ortega describe real systems that are used to find fraud, they cannot go into detail about the exact workings of the systems. Doing this would give fraud perpetrators an advantage in penetrating the fraud defense. This paper belongs to this third category and focuses on building data views and applied techniques for predictive analytics based on Sparrow's seven levels of fraud control.

5.4 A Multidimensional Data Model and Analysis Techniques for Fraud Detection

5.4.1 A Medicaid Multidimensional Schema

This section describes the design of a multidimensional schema that, based on Medicaid data, will underpin this analysis and allow for the creation of different views of that data that address Sparrow's classification of fraud types. Medicaid providers use four different claim forms to submit claims to the source system: CMS1500 for outpatient professional services, J400 for dental services, UB-04 for institutional claims, and the Drug Claim Form for pharmacy claims. These claims vary slightly in the information collected by purpose, but the general data structure is similar, defining who did what to whom, when, and why. To maintain the data granularity and specificity, four different claim types: inpatient, long-term, pharmacy, and professional will be introduced. It should be noted that, as the data is specific to the type of service provided, most commercial insurance claims follow a similar template.

A general core that each claim exists of can be extracted among the different claim forms: patient, provider, diagnoses, procedures, and amounts charged. In this model, the fact table represents a single line from a claim to offer the most flexibility to the user. For each claim line, a type field links to type-specific detailed information. Based on the desired views from the last section, the following dimensions are included: date (claim filed, service, paid), provider (executing, referring, billing), patient, insurer policy, treatment, diagnosis, claim type, drug, outcome, and location. The following numeric facts can be distinguished, some computed by the other facts: Covered charges ($), Non-covered charges ($), Total charges ($), Units of service, Number of days between claim filled and paid, Number of days between service and claim paid, Distance between provider and patient, Number of days between service and claim filled, Covered price per unit, Total price per unit, and Treatment duration. Figure 13 shows the resulting multidimensional schema.

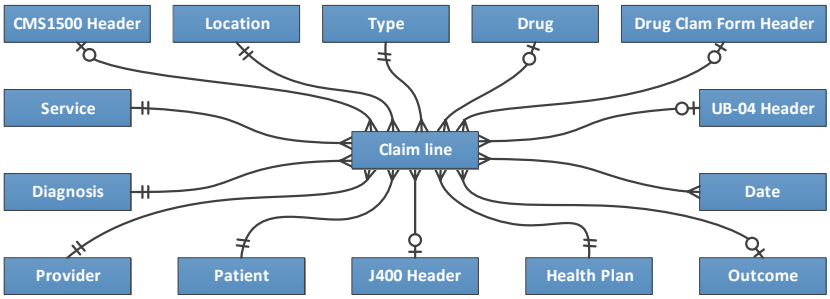


Figure 13 - Medicaid Multidimensional Schema

5.4.2 Data Models Addressing Levels of Fraud

Based on the Medicaid environment and available knowledge base, multidimensional data models representative of Sparrow's fraud classifications and accompanying analysis techniques for detecting the most prevalent fraud types at each level were developed.

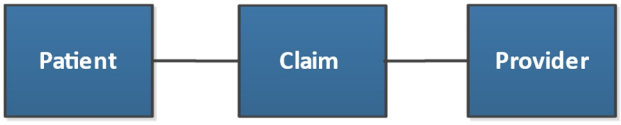


Figure 14 - Level 1 Entities -- Single Claim or Transaction

Level 1 depicts what today's claims processing systems see: a single claim with its relevant patient and provider. Typically, decisions possible at this

level are programmed as edits in the claims processing system to prevent fraud. Using this level, for example, one can reject duplicate services on a claim and check to see that services are consistent with diagnosis code(s).

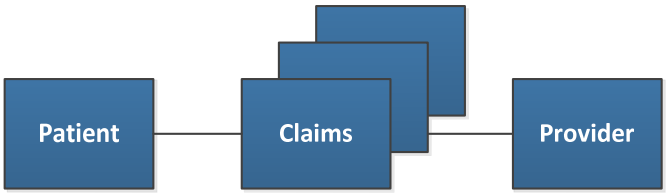


Figure 15 - Level 2 Entities -- Patient / Provider

Level 2 focuses on the relationship between a patient and a provider, including all claims billed. Duplicate billing can be flagged by checking all claims for duplicate providers, patients, and service dates. Unbundling could be discovered by looking for multiple services from the same provider across claims that should have been grouped. Excessive or unnecessary services could surface when care patterns do not match diagnoses.

Figure 16 - Level 3a Entities -- Patient

Level 3a shows all claims and providers treating a single patient. Phantom billing could be discovered by examining the patient's claims vs. prior medical history. How does the patient's temporal claims pattern compare with other patients? One could search for unreasonable claims, such as medically impossible services given known history or services on the same day at two locations far apart. This is the best place to see duplicate billing, checking for all claims for duplicate service performed on the same date across all providers. Upcoding could be discovered by looking at claims across providers for consistency. For example, a cardiologist billing for a complicated open-heart surgery and an anesthesiologist billing for a simple procedure on the same service date is suspicious. Unbundling schemes could also surface by analyzing multiple providers providing components of a bundled service to one patient. Excessive or unnecessary services across

providers can be found by comparing the patient's service pattern with others with similar diagnosis codes. One can also identify groups of providers through utilization coincidence across patient profiles at this level. These groups are essential in detecting more complex fraud schemes in 4b and 6b.

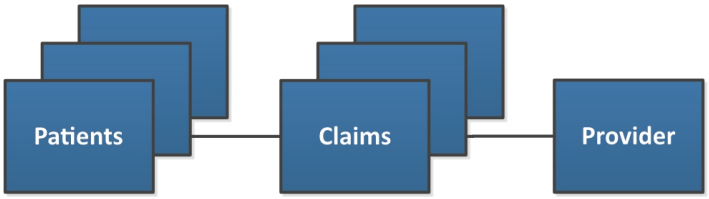


Figure 17 - Level 3b Entities -- Provider

Level 3b exposes the provider. A wealth of knowledge can be gained by analyzing the provider's service distribution and frequency against peers. Clustering analysis of these profiles shows clusters of specialists. Medical subject matter experts should evaluate distribution and frequency outliers for legitimacy. Geospatial analysis of patient distance to the provider in this model adds additional detail. This is one of the best views to spot phantom billing, upcoding, unbundling, and excessive or unnecessary services.

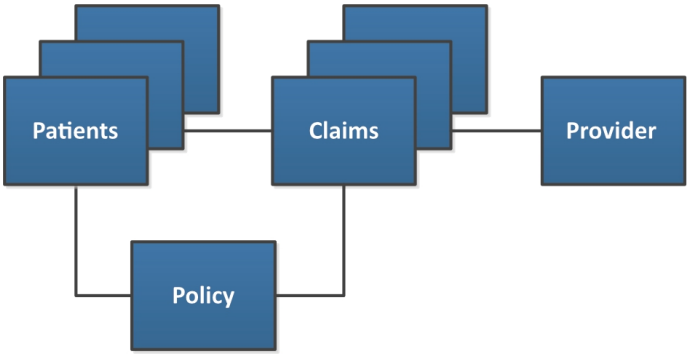


Figure 18 - Level 4a Entities -- Insurer Policy / Provider

Level 4a analyzes claim pattern differences across different insurance policies or insurers. This could expose providers targeting specific insurers. Patient distributions across insurers tell a story, as most providers have a diverse patient base. Providers with high proportions of patients and claims billing specific programs, especially government ones, should be evaluated closely. Phantom billing, upcoding, unbundling, excessive or

unnecessary services, and kickbacks could surface with this analysis. Unfortunately, multiple insurer data is rarely available for this analysis.

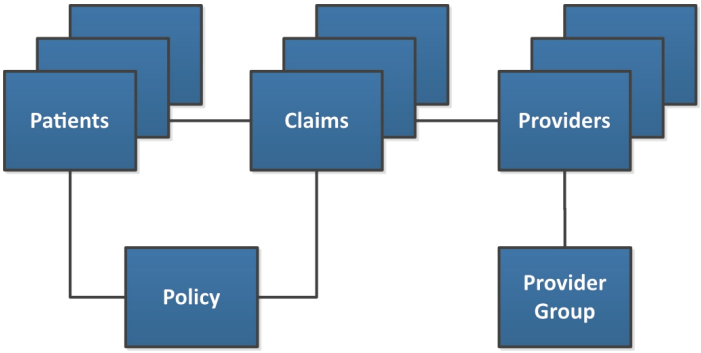


Figure 19 - Level 4b Entities -- Patient / Provider Group

Level 4b looks at all claims for one patient across a known group of providers, such as a typical clinic. Here, fraud schemes directed within the group and spread amongst providers may stand out. Level 6b is a more effective model for analyzing more complex schemes, and 3a and 3b cover simpler methods.

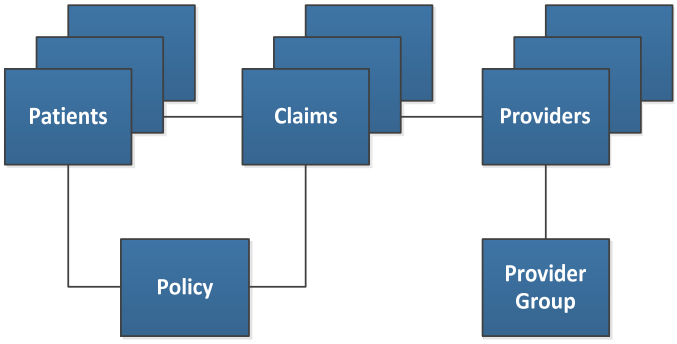


Figure 20 - Level 5 Entities -- Insurer Policy / Provider Group

Level 5 combines levels 4a and 4b, showing policy-based variations in a provider group's services. This should be used to evaluate the provider group's insurance billing distribution compared with their peers' distribution with a similar patient demographic sampling. Referral patterns may also show policy-specific variations that could be explainable or not. Similar or identical service patterns from the same providers in the group to many patients varying by insurance should be evaluated for reasonableness.

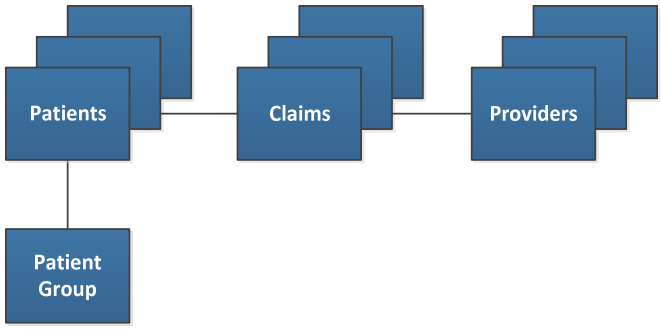


Figure 21 - Level 6a Entities -- Defined Patient Group

Level 6a focuses on patient groups, such as residents of a typical nursing home. Here, one would compare claims profiles for patients within the group to similar individuals outside the group. Are the services claimed normal demographically? Are certain providers disproportionately servicing this group with services not commonly needed in the environment? For example, does every patient receive orthotic shoe inserts from a provider? This may seem normal when looking at a DME provider alone in 3b, but overlaying the patient group in 6a disproportionately connects these patients and highlights possible excessive or unnecessary services. Numerous shared patient mailing addresses, projected here in a patient group, could point to identity theft where a billing provider has changed the patient's address to phantom bill.

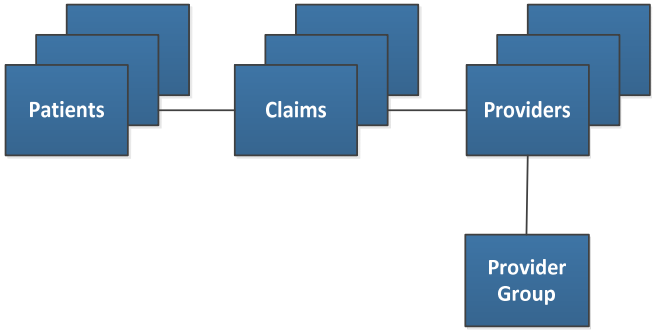


Figure 22 - Level 6b Entities -- Provider Group

Level 6b looks at all claims across a known provider group. Since providers work together and can also bill individually or through clinics or hospitals, this is one of the most useful views of the data. Clustering analysis of the group's service distribution will highlight like groups and identify outlier

groups for further study. Link analysis of referrals and prescriptions, along with frequency comparisons with similar provider groups, can help detect excessive or unnecessary services that cross provider lines but enrich the group.

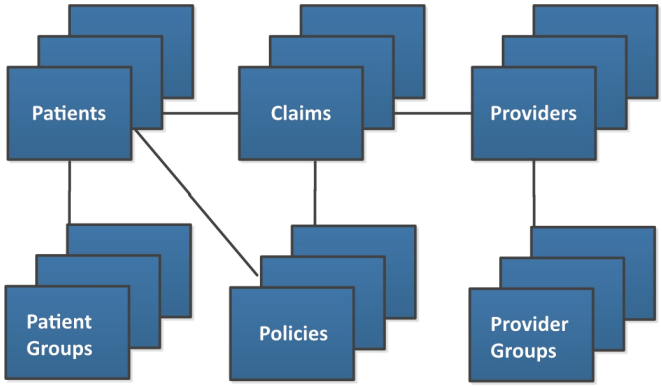


Figure 23 - Level 7 Entities -- Multiparty, Criminal Conspiracies

According to Sparrow (2000), the "art of detection at this level involves watching for broad patterns of coincidence or connection between hundreds or thousands of otherwise innocuous transactions." Level 7 combines all previous data views and concerns all fraud that is part of criminal networks, which involve many different beneficiaries and providers. This much larger data view, spanning billions of claims in the case of Medicaid, is the richest, delivering the ability to perform complex network analysis that could detect intricate conspiracies. However, the analysis performance here will be much lower than in previous levels. So, it is best for targeted analysis that could not be performed in lower-level views.

5.4.3 Using the Views to Detect Fraud

As discussed at each level, the analyst needs to know where to look to find specific kinds of fraud. Table 7 provides a typology mapping the six most common types of fraud to the levels at which they will most likely be found.

		Phantom Billing	Duplicate Billing	Upcoding	Unbundling	Excessive, Unneeded Services	Kickbacks
Level 1	Single Claim, or Transaction				*	*	
Level 2	Patient / Provider		*		*	*	
Level 3	a. Patient	*	***	*	***	*	
	b. Provider	**		***	*	***	
Level 4	a. Insurer Policy / Provider	**		*	**	**	*
	b. Patient / Provider Group	*	*	*	*	*	
Level 5	Insurer Policy / Provider Group	**		**	**	**	*
Level 6	a. Defined Patient Group	**		*	*	**	**
	b. Provider Group	**		***	**	***	*
Level 7	Multiparty, Criminal Conspiracies	**		**	*	**	***

Usefulness: * Low ** Medium *** High

Table 7 - Level Usefulness in Detecting Prevalent Fraud Types

5.5 Evaluation

The model and process were evaluated by subjecting them to recent healthcare fraud cases. This section maps these real-world cases against the data models and methods suggested in this paper to test whether the fraud could be detected.

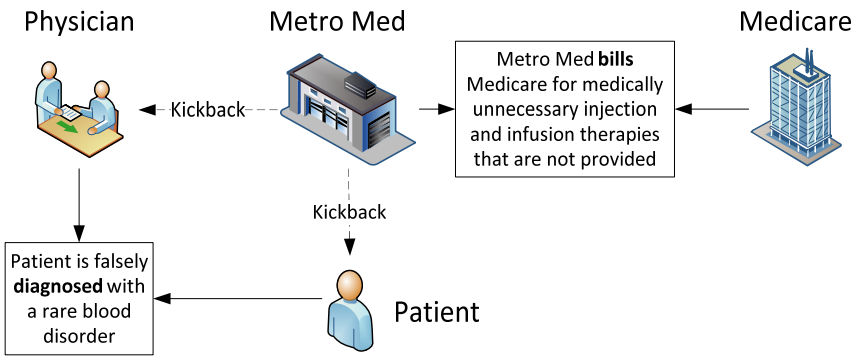


Figure 24 - Case 1: HIV Injection and Infusion Medicare Fraud Scheme

In a case published by the United States Department of Justice (Department of Justice, 2011), a physician, Rene De Los Rios, was convicted of five felony fraud counts for her part in a Medicare fraud scheme,

defrauding the government of $23M in collusion with an HIV infusion clinic, Metro Med. In 2003, Metro Med began operating as an HIV infusion clinic that purportedly provided injection and infusion therapies to HIV-positive Medicare beneficiaries. These services were medically unnecessary and not delivered. Metro Med paid cash kickback payments to patients for their collusion. De Los Rios was paid to be the licensed physician who would order tests, sign medical forms and charts (often never seeing a patient), and make it appear that legitimate medical services were being provided. He diagnosed almost all the patients with the same rare blood disorders to maximize Medicare reimbursements and prescribed expensive medications, such as Winrho, Procrit, and Neupogen, to further bill Medicare. Metro Med paid the defendant $3,000 weekly for his scheme involvement. Figure 24 visualizes this scheme.

The scheme includes multiple types of fraud, including phantom billing, medically unnecessary services, and kickbacks. One could compare physician service profiles with their peers using the level 3b data model to detect this and similar schemes. Dr. De Los Rios's excessive diagnosis of a rare blood disorder and abnormal, expensive prescriptions would have been an outlier that could have pointed to this problem. Identifying these patients as a suspect patient group, level 6a would show the other providers (the clinic and possibly more) that could be involved in this scheme.

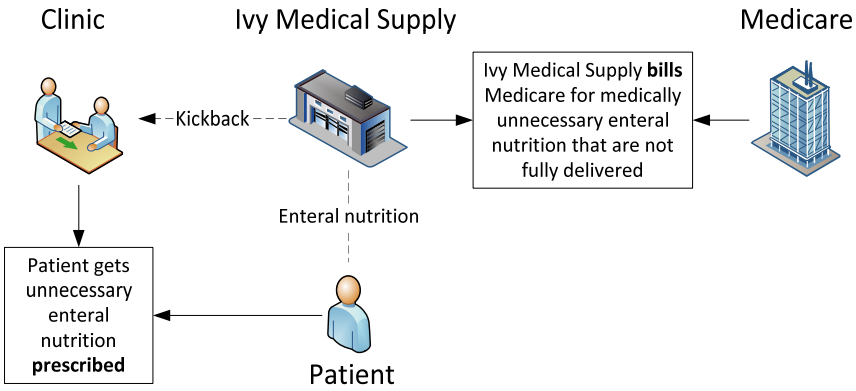


Figure 25 - Case 2: False claims to Medicare for durable medical equipment

In another case (United States Attorney's Office for the Central District of California, 2012), California doctors and colluding durable medical

equipment (DME) suppliers allegedly submitted over $5M in false claims to Medicare. The defendants prescribed and billed for enteral nutrition, a liquid nutritional supplement provided via a feeding tube directly into the stomach, duodenum, or jejunum. The doctors, Dr. Augustus Ohemeng and Dr. George Tarryk, wrote fraudulent prescriptions for patients who did not have feeding tubes. George Laing, who managed the clinic where Tarryk and Ohemeng practiced, allegedly received kickbacks in exchange for referring the prescriptions to Ivy Medical Supply. Ivy then fraudulently billed Medicare for the enteral nutrition, even though it was not medically necessary and was not delivered to patients in the quantities billed to Medicare.

This scheme also includes multiple types of fraud, including phantom billing, medically unnecessary services, and kickbacks. Using level 3a, comparing the service pattern of these patients with their peers would highlight that their patients were not previously billed for surgically inserting a feeding tube. This could be explained if the feeding tube was inserted while enrolled in a different health insurance, but the cluster of these patients would stand out, nonetheless. Linking these patients together to look at their servicing providers would highlight the actors involved in this scheme. Alternately, abnormally high prescribing patterns for enteral nutrition could be seen in level 3b when comparing the prescribing patterns of the two doctors to their peers. Identifying these patients as a suspect patient group, level 6a would show the other providers (the clinic and possibly more) that could be involved in this scheme.

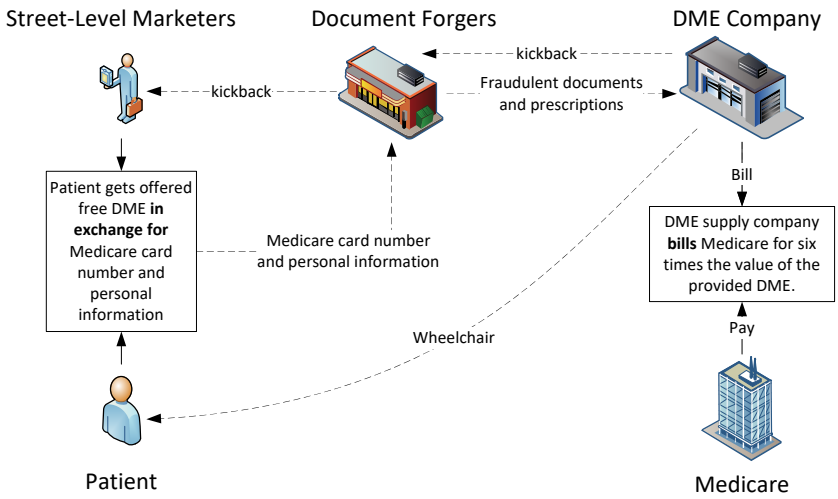


Figure 26 - Case 3: Billing Medicare for unnecessary, expensive, high-end power wheelchairs and orthotics

A 2012 case involving $14.2M in Medicare fraud (Department of Justice, 2012) showed a DME company purchased fraudulent prescriptions and patient information to fraudulently bill Medicare for expensive, high-end power wheelchairs and orthotics that were medically unnecessary or never provided. Company owners hid the money they used to pay for these fraudulent prescriptions by writing checks to a third shell company called "Direct Supply." The checks would then be cashed, and the money would be used to pay kickbacks to street-level marketers offering free power wheelchairs and other DME in exchange for Medicare IDs and personal information. This information would then be used to create fraudulent prescriptions. As depicted in Figure 26, this scheme includes multiple types of fraud, including phantom billing, upcoding, medically unnecessary services, and kickbacks.

This fraud scheme is complicated to detect due to the number of actors and likely multiple (faked) prescribing physicians. However, the model may uncover this fraud over time through various analyses:

- Level 3b: Is the DME provider's service distribution abnormal compared to peers? Only billing for high-end wheelchairs may stick out, though it could be explained if the company only sold high-end models.

- Level 3b: Is the company showing unnatural growth patterns? Businesses are built to grow and can do so quickly, but does this agree with the multitude of prescribing physicians? Put another way, a business usually grows quickly by taking on a large customer/referrer, such as becoming the preferred supplier for a hospital vs. tens or hundreds of independent prescribing physicians. This aberrance may show up.
- Level 3a: A third and more telling indicator could come from the analysis of the patient temporal claims patterns compared with other patients. The fact that these patients did not have prior mobility-related claims should set them apart from their peers. Then, analyzing the suspect patient group using level 6a would show the other providers (the clinic and more) that could be involved (the common DME supplier) or compromised (the supposed referring physicians) in this scheme.

5.6 Conclusions

The design science contribution was structured according to the Hevner et al. (Hevner et al., 2004) model. The research addresses a relevant and important problem in Medicaid healthcare fraud detection. This paper offers artifacts, including a set of multidimensional data models and analysis techniques for healthcare fraud detection, along with a projection of these models to a Medicaid-specific schema that would accommodate this analysis. The artifacts are evaluated by discussing their potential in detecting three healthcare fraud cases. The paper contributes to the literature by mapping the different levels of Sparrow(Sparrow, 2000) to a set of multidimensional data models and analysis techniques applicable at each level for fraud detection. The representation of the artifact used data modeling as a construction method and was evaluated to a list of the most prominent healthcare fraud types. The domain context of Medicaid and discussed different design alternatives were utilized. The model was communicated to stakeholders in Medicaid, including applying the multidimensional schema in practice.

Through this research, many lessons were learned about antifraud efforts. Significant healthcare subject matter expertise is required to design analysis techniques and interpret their results. Potential entity

relationships, medical necessity, and legitimacy in the context of finding the unknown unknowns are extremely difficult to model comprehensively. The artifacts provide a roadmap for an analyst to evaluate the detected patterns. Lack of training data (marked fraudulent claims) complicates the application of supervised techniques today. It is envisioned that, as models such as these are applied and used by fraud analysts in a structured environment, training data can be developed based on analyst decisions around likely fraudulent and appropriate claims, further enriching the data and opening doors to supervised techniques. The quest to identify the unknown unknowns in healthcare fraud will never end. Still, with structured data models, analysis techniques, and continual feedback, we can advance the state of the art in fraud detection and make inroads into a significant societal challenge.

6

Chapter 6: Outlier Detection in Healthcare Fraud: A Case Study in the Medicaid Dental Domain

Adapted from:

Dallas Thornton, Guido van Capelleveen, Mannes Poel, Jos van Hillegersberg, Roland M. Mueller, 2014. Outlier-based health insurance fraud detection for U.S. Medicaid data. Proceedings of the 16th International Conference on Enterprise Information Systems, pp. 684–694.

Guido van Capelleveen, Mannes Poel, Roland M. Mueller, Dallas Thornton, Jos van Hillegersberg, Outlier detection in healthcare fraud: A case study in the Medicaid dental domain, Int J Account Inf Syst (2016)

Chapter 6: Outlier Detection in Healthcare Fraud: A Case Study in the Medicaid Dental Domain

6.1 Summary

This chapter illustrates the application of unsupervised outlier techniques at the post-payment stage, aiming to uncover fraudulent patterns within received insurance claims. Special attention is given to the system's architecture, the development of metrics for outlier detection, and the identification of potentially fraudulent providers, all crucial in aiding fraud experts in their evaluations and investigations.

The algorithms were tested using Medicaid data, which included 650,000 healthcare claims and 369 dentists from a specific state. Upon evaluating the flagged cases by two healthcare fraud experts, it was determined that 12 out of the top 17 providers (accounting for 71%) exhibited suspicious claim patterns, warranting further investigation by officials. Conversely, the remaining five providers (29%) were deemed potential misclassifications, as their patterns could be justified by unique characteristics of the provider's practice.

By selecting and scrutinizing the top flagged providers, this approach has proven effective for targeting and identifying instances of potential fraud. An in-depth analysis of individual providers revealed certain cases that could be fraudulent. The study concludes that outlier detection is a powerful tool that can unveil new patterns of potential fraud, which could be integral in enhancing future automated detection mechanisms.

6.1 Introduction

This chapter uses a multi-dimensional data model for Medicaid claim data (Thornton et al., 2013) and a seven-step methodology (Thornton et al., 2014) in a detailed case study of outlier detection applied to one state's Medicaid dental claims. This contributes to the literature by showing how outlier techniques can be used in healthcare to target potentially fraudulent activity. It shows that, through outlier detection, new patterns of potential fraud can be identified and potentially utilized in future automated detection mechanisms.

6.2 Research Domain

The section describes the related literature on data mining for medical fraud detection. Second, medical fraud is put in the context of the Medicaid program—the claim processing is described, and an outline of the current fraud detection mechanisms is given.

6.2.1. Related Work

The integration of technological advancements, digitization of healthcare information, and extensive research on health insurance fraud have catalyzed the adoption of data mining and machine learning in the fight against fraud. Researchers utilize data mining for fraud detection (Aral et al., 2012), and electronic fraud detection systems hold the potential to improve the integrity of claims processing. These systems scrutinize claims, identifying irregularities during pre-processing and searching for fraud indicators post-processing (Aral et al., 2012; Bolton & Hand, 2002; Forgionne et al., 2000; Ortega et al., 2006).

However, the healthcare sector significantly trails behind industries such as banking and telecommunications in adopting statistical analysis and data mining techniques (Travaille et al., 2011). This slow adoption can be attributed to the healthcare industry's complexity, fragmented claims processing systems, and inadequate political support and funding for fraud detection initiatives (Sparrow, 2000).

Although previous research has identified data mining applications for uncovering fraud schemes (Forgionne et al., 2000; Major & Riedinger, 2002; Musal, 2010; Ng et al., 2010; Shin et al., 2012), extending these applications to a more extensive and more diverse medical domain for effective utilization by fraud experts remains a significant challenge.

A thorough review of data mining-based fraud detection research highlights these challenges and suggests alternative data sources and solutions from related fields (Phua et al., 2010). Initially, outliers were recognized as a basic form of anomaly detection, valuable for validating data quality and detecting accidental errors and potential fraudulent patterns (Bolton & Hand, 2002). While outlier detection techniques offer opportunities for supervised learning, the prevailing advocacy for hybrid or unsupervised methods stems from the scarce availability of fraudulent

cases for training, ever-changing program policies, and evolving fraud schemes.

In the early 2000s, the healthcare sector saw a surge in the adoption of data warehousing for fraud detection (Forgionne et al., 2000). Intelligent systems combining data mining, artificial intelligence, and decision support systems were developed to detect healthcare fraud proactively. Notable larger-scale applications include a project reviewing 20,000 providers based on 27 behavioral heuristics, identifying 91 potentially fraudulent cases out of 900 flagged instances (Major & Riedinger, 2002).

Experimental applications have also been explored. For instance, outlier detection algorithms were used on pathology insurance data in Australia, revealing several rare cases (Yamanishi et al., 2004). In Canada, Benford's Law was employed to detect anomalies in claim reimbursements, although its effectiveness was limited due to the nature of the services and fixed prices by payers (Lu & Boritz, 2005). In Taiwan, a process mining framework was developed within the National Health Insurance program to detect fraudulent claims, with the detection model capturing an average of 69% of fraudulent and abusive cases (Yang & Hwang, 2006).

In Chile, neural networks were utilized by a private health insurance company to detect medical fraud and abuse, processing claims in real time and achieving a significant detection rate (Ortega et al., 2006). Similarly, Medicare Australia employed association rule mining to scrutinize billing patterns within specific specialist groups, resulting in more effective identification of suspicious billing patterns than random sampling (Shan et al., 2008). Additional efforts in Medicare Australia focused on identifying prescription shoppers using spatiotemporal health data and multiple metrics (Ng et al., 2010; Tang et al., 2011). Although these methods showed promising results, the benefits of spatiotemporal factors over traditional metrics could not be conclusively determined.

In the United States, researchers developed models using clustering and regression for geographical analysis to investigate Medicare fraud (Musal, 2010). Another study outlined a straightforward methodology to pinpoint and prioritize potential targets for auditing prescription fraud (Iyengar et al., 2014). The researchers established a standard behavioral model for

each category of prescription, against which they compared actual data to identify statistically significant deviations. In specific categories, they considered up to 500 characteristics to detect irregularities. Impressively, in the category of narcotic analgesics, the model successfully identified all verified instances of fraud, flagging them as highly abnormal and excessive.

Further investigations were carried out in Brazil, where a model was proposed to assess provider behavior, utilizing k-means clustering to identify outliers and detect excessive billing (Hillerman et al., 2015). Another study outlined a seven-step process to evaluate the efficacy of mining healthcare data for fraud detection (Joudaki et al., 2015).

Overall, previous research has validated the applicability of data mining techniques in detecting healthcare fraud across various medical insurance sub-domains, increasing industry awareness and demonstrating potential benefits. However, challenges remain in applying these techniques universally to assist fraud experts. The ever-evolving nature of fraud, the complexity of the health insurance domain, and the intricate structure of insurance policies and state regulations present significant hurdles. This chapter delves into applying unsupervised outlier techniques at the post-payment stage, providing a nuanced approach to identifying fraudulent health insurance claims.

6.2.2 Medical Fraud

Understanding the complexities of the medical insurance industry, claim processing, and potential fraud schemes is crucial for fraud detection. Fraud is "the intentional act of deception or misrepresentation made by an individual, who knows it to be false or does not believe it to be true, with the intention of gaining unauthorized benefits for themselves or others" (Department of Health and Human Services, 2012). In the context of Medicaid, three main groups are susceptible to committing fraud: patients, insurers, and providers (Li et al., 2008). This chapter primarily focuses on providers, who are central in initiating fraud schemes by submitting fraudulent billings to insurers. However, it is essential to acknowledge that other parties can also engage in fraudulent activities.

Addressing fraud requires acknowledging the challenges posed by the inherent uncertainties and inconsistencies in medical care (Henderson,

2014). Furthermore, healthcare fraud is a dynamic issue, constantly evolving as detection methods improve. As new safeguards are implemented, those engaged in fraudulent activities adapt, seeking new avenues to exploit system vulnerabilities. Typical healthcare fraud schemes include billing for services that were never provided, upcoding (inflating bills by using codes for more expensive services), submitting duplicate claims, unbundling claims (billing for each component of a service rather than the bundled rate), and providing unnecessary or irrelevant medical services (Sparrow, 2000).

6.2.3 Medicaid Claim Process

Providers participating in Medicaid receive reimbursement directly from the state or a managed care entity for submitted claims. On the other hand, non-participating providers send bills directly to patients, who must then pay and subsequently request partial reimbursement from Medicaid or the state Medicaid insurer. In both cases, the agency or insurer processes the claim and issues an Explanation of Benefits (EOB) to the patient. The EOB details the services, associated codes, and costs.

Claims processing systems conduct various prepayment checks and edits to assess a claim's legitimacy, as Sparrow (2000) outlined. These checks include validating forms, ensuring proper procedure codes are used, verifying pricing, and preventing duplicate submissions. However, these systems cannot verify whether the services were provided, if the diagnosis was correct, or if the patient is even aware of the claimed services. As a result, fraudulent claims can potentially pass through these checks.

EOBs, although designed to offer protection against fraud, currently provide minimal security (Sparrow, 2000). Beneficiaries have little financial incentive to scrutinize complex, computer-generated forms and billing codes, especially when they do not have a balance due. Furthermore, fraudulent schemes often target vulnerable Medicaid populations, such as the homeless, mental health patients, and individuals with disabilities. These groups may struggle to understand the EOB, or they might receive kickbacks from providers to remain silent (Kelley, 2009).

Fraud prevention and detection initiatives in Medicaid are typically organized at the state level and managed by agencies and claims

processing contractors. Fraud is primarily detected and addressed through audits, which can be randomly selected or triggered by inconsistencies in submissions or structural monitoring. Despite these efforts, the system largely depends on cases filed under the False Claims Act (Department of Health and Human Services and Department of Justice, 2014). The use of fraud analytics in Medicaid is increasing (Centers for Medicare and Medicaid Services, 2014), with experts advocating for the intensification of electronic fraud detection. Such methods can enhance security during the claim input process, check for irregularities, and analyze claims to identify potential indicators of fraud (Aral et al., 2012; Bolton & Hand, 2002; Forgionne et al., 2000; Ortega et al., 2006).

6.2.2 Dental Claims Fraud

Despite the annual expenditure of over $100 billion on dental services in the United States, there is a scarcity of literature addressing the issue of dental claims fraud. Dentistry comprises a substantial and relatively uniform group of service providers, making it an ideal candidate for peer group analysis. In this case study, there was access to dental domain expertise, allowing for the evaluation of metrics and results with the guidance of subject matter experts.

6.3 Method for Applying Outlier Detection to Healthcare Fraud

To effectively manage the need for ongoing review, adjustment of metrics, and modifications to the weighting of different factors, we propose a comprehensive iterative process specifically designed for applying outlier detection in healthcare fraud scenarios, as illustrated in Figure 27. The following subsections provide detailed descriptions of each phase within this process.

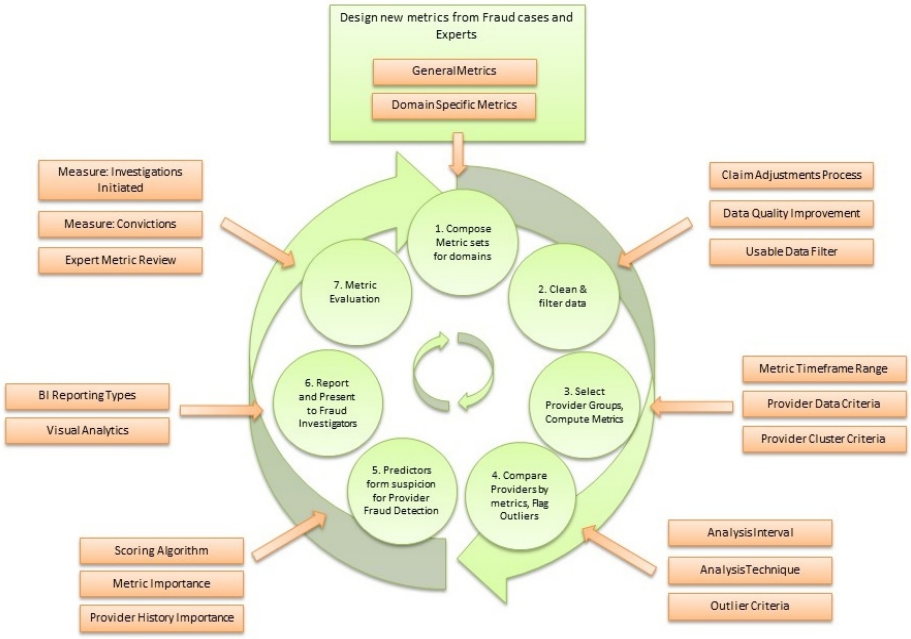


Figure 27 - Method for Applying Outlier Detection to Healthcare Fraud

6.3.1 Compose Metric Sets for Domains

Metrics can be developed through various methods, including case analysis, literature review, examination of data model attributes, or collaboration with industry experts. While case studies can aid in creating a metrics set, evaluating these metrics through expert opinions and analyzing the flagged results is crucial. The metrics selected for our case study were derived from various sources, including cases identified through the FBI news blog (U.S. Federal Bureau of Investigation, 2013), discussions with healthcare fraud experts, and existing literature (Musal, 2010; Ng et al., 2010; Shin et al., 2012; Tang et al., 2011; U.S. Government Accountability Office, 2012).

To illustrate the process of extracting fraud metrics, consider the following two examples:

1. In New Jersey, a physician and owner of a home-based physician services firm for seniors admitted to charging for lengthy visits never provided to elderly patients (District of New Jersey U.S.

Attorneys Office, 2013). The physician, who received at least half a million dollars, was eventually caught due to being the highest billing home care provider among over 24,000 doctors in New Jersey from January 1, 2008, to October 14, 2011. This case highlights upcoding—intentionally overbilling for services—a behavior detectable through metrics. A metric could be designed to compare providers based on the proportion of lengthy patient visits, potentially identifying providers who fraudulently claim such visits.

2. In Texas, a doctor at a community medical center was involved in fraudulent activities by misrepresenting office visits and unnecessary diagnostic tests from February 2010 to February 2011 (District of Texas U.S. Attorneys Office, 2013). Patients were prescribed controlled substances in return for undergoing diagnostic tests, creating an incentive for repeated visits. This fraudulent scheme could be detected through metrics evaluating referral rates, types and amounts of specific tests prescribed, or patient retention and visit frequency.

Developing metrics for fraud detection requires a deep understanding of the healthcare domain and statistical theory. The design process goes beyond analyzing fraud cases to uncover potential fraud indicators. It is essential to recognize that a group of outliers identified through a single metric inevitably includes some cases that deviate purely by chance. To effectively separate fraudulent providers from non-fraudulent ones, it is crucial to iteratively refine the set of metrics based on expert input and continuous evaluation.

The number of metrics used does not need to be extensive. Data mining literature suggests using between 25 to 30 features or item sets. Employing excessive metrics can lead to many outliers, potentially categorizing all providers as displaying outlying behavior in some metrics. A balanced and effective set of metrics can be achieved through iterative cycles of evaluation and adjustment.

Metric identification relies heavily on the expertise of fraud detection specialists and is an iterative process aimed at refining the set of metrics for optimal effectiveness.

6.3.2 Clean and Filter Data

This phase focuses on preparing and refining the dataset to ensure its suitability for analysis. This involves cleaning the data to minimize measurement uncertainties and selecting only the relevant data related to the providers under investigation.

The first step is to assess and enhance data quality, which is crucial for ensuring the precision of subsequent computations. Various factors can compromise data quality, and three primary concerns need to be addressed:

- Data Integration: Frequently in Knowledge Discovery in Databases (KDD) and Decision Support Systems (DSS), particularly in large commercial and governmental organizations, there is a need to merge multiple databases containing information about common entities. This process can introduce inconsistencies and errors (Hernández & Stolfo, 1998).
- Data Entry Quality: Manual data entry makes Health insurance data susceptible to quality degradation. Studies have shown that data entry errors can occur in approximately 4.4% of cases involving personal information, with even higher error rates in more complex data abstraction tasks (Colin et al., 1994).
- Data Accuracy: Claims are sometimes initially submitted with errors and adjusted afterward. If possible, any claims that have been submitted incorrectly should be identified and removed from the dataset.

Data cleansing is a highly recommended preliminary step. This process involves detecting and correcting (or removing) corrupt or inaccurate records from the dataset, ensuring its integrity.

After cleansing, the next step is filtering, which involves selecting only the data suitable for analysis. Any data that contains missing values, rendering it unsuitable for metric calculation, should be removed. Additionally, any claims that have been voided or otherwise invalidated should be filtered out of the dataset.

The goal is to ensure that the dataset, particularly the claim transaction data, meets the ISO 8000 data quality criteria to the greatest extent

possible before proceeding with the analysis. This sets the stage for accurate and reliable results in the subsequent phases of the fraud detection process.

6.3.3 Select Provider Groups, Compute Metrics

For a meaningful comparison of providers' behaviors, they should share similarities. The primary challenge is striking a balance between homogeneity and sample size. When providers are more alike in a group, outliers become more apparent. However, this homogeneity may result in a smaller sample size. This raises three critical considerations:

- Data Quantity: Is there a minimum number of data points required for a provider to be included in the analysis? For instance, a provider with only two claims per month might not provide enough data for meaningful comparisons and could be excluded.
- Sample Size: What is the smallest number of providers in a group that can yield reliable comparisons? For example, a group comprising only five providers may not offer reliable insights due to its limited size.
- Provider Characteristics: What criteria can be used to group similar providers for comparison? While operating in the same domain or sub-domain is a given, other characteristics, such as the size of the provider or the volume of patients they handle, can influence the outcome. If a cluster analysis is conducted to identify these nuances, the criteria used in the clustering can aid in defining these groups.

Once metrics are ready for analysis, they are calculated and stored. Defining the timeframe over which each metric will be analyzed is essential. In the study mentioned, a specific timeframe was chosen, with provider behaviors being assessed based on the predefined criteria for each metric.

6.3.4 Compare Providers by Metric, Flag Outliers

The interval and frequency for analysis and metric computation need specification. In scenarios where new data is uploaded monthly, a pragmatic approach would be to conduct monthly metric calculations and

analyses. This strategy should be chosen carefully considering the required computational resources and the availability of subject matter experts.

Following this, appropriate analytical techniques and outlier detection methods must be selected for each metric. In the experiment mentioned earlier, various analysis methods were employed, including univariate, multivariate, time-series, and box-plot analyses. A range of methods was applied to detect outliers, such as deviations from the regression model, deviations within clusters, individual deviations from clusters, trend deviations, and peak deviations. These methods incorporated non-parametric approaches (which do not assume an underlying statistical distribution) and parametric approaches (which utilize Gaussian mixture models to identify outliers).

6.3.5 Predictors Form Suspicion for Provider Fraud Detection

A crucial consideration is the method of reporting anomalies and linking them to potential fraud indicators. When a provider surpasses a predefined outlier threshold, an alert is triggered for that specific period. This alert, or "flag," signifies an anomaly identified by the data mining algorithm, commonly known as the outlier. The scoring process takes these flags and computes a fraud suspicion level based on each outlier detected during the provider analysis.

The proposed scoring system essentially accumulates suspicion levels. A singular provider analysis might inadvertently flag legitimate providers. However, the rationale behind using a scoring system is to highlight those providers who consistently appear as outliers across various indicators. The idea is that providers frequently flagged across multiple metrics are more likely to warrant further investigation for potential fraud.

6.3.6 Report and Present to Fraud Investigators

Fraud investigators require a versatile approach to reporting, as there is no one-size-fits-all method for presenting the data. A combination of dashboards and interactive multidimensional processing is advised to cater to this need.

Dashboards serve to provide high-level information on providers. This includes showcasing metric results for each provider, highlighting deviations from typical patterns, and flagging providers that exhibit

abnormal behavior either in comparison to others or based on their historical data.

For a more in-depth analysis, investigators can utilize comparative analysis tools. These tools allow them to delve deeper into specific claims, aiding in the identification of how particular deviations may have occurred. This process helps in compiling a list of claims that necessitate further scrutiny.

A helpful starting point for investigators could be a curated list of alerts and their respective scores. This approach streamlines the initial phase of the investigation, directing attention to areas of potential concern based on the accumulated data.

6.3.7 Metric Evaluation

Evaluating the efficacy of predictors is crucial for refining analyses and enhancing metric development. However, determining "success" is challenging, as an act is not officially labeled as fraud until post-litigation, which can take years. Hence, relying on convictions as a basis for resource allocation or to inform iterative improvements can be inefficient. A more immediate and potentially reliable measure might be the number of investigations and audits initiated by fraud experts after an internal review.

Should the initiation of fraud investigations be used as an evaluation metric, precision and recall formulas can be applied to gauge the effectiveness of the detection method. However, this approach has its drawbacks. There is a risk that investigations could be consistently initiated based on incorrect premises, thereby skewing the effectiveness measurements. While fraud convictions could later contradict these findings, seasoned fraud experts can provide valuable insights into these metrics.

The configuration of outlier detection algorithms, particularly their thresholds, affects how data points are classified as outliers. A conservative approach may overlook potential frauds, while a more liberal one might produce false alarms. Striking the right balance is essential, and this trade-off can be assessed using precision and recall metrics, as Aggarwal (2013) suggested.

$$\text{Precision(t)} = 100 \cdot \frac{|S(t) \cap G|}{|S(t)|}$$

$$\text{Recall(t) or TPR(t)} = 100 \cdot \frac{|S(t) \cap G|}{|G|}$$

The set of providers is represented as S(t), where 't' indicates the threshold or criteria for identifying outliers. The providers that are accurately classified as outliers, known as the true set or ground truth, are represented by G. By plotting the True Positive Rate (TPR(t)), also known as recall, alongside the False Positive Rate (FPR(t)), we can determine the optimal criteria for identifying outliers. The False Positive Rate (FPR(t)) represents the proportion of false positives (providers incorrectly identified as outliers) out of all the true negatives (providers correctly identified as non-outliers). The formula for FPR(t) is as follows:

$$\text{FPR(t)} = 100 \cdot \frac{|S(t) - G|}{|D - G|}$$

6.4 Outlier Detection in Dental Claims

To implement this method for detection, the following steps were taken:

- Identification of Potentially Relevant Metrics: A thorough review of existing literature was conducted to pinpoint potentially significant metrics for our analysis.
- Compilation of a Representative Data Set: A data set representative of the situation was meticulously assembled to evaluate the pertinence and effectiveness of the identified metrics.
- Evaluation through Expert Interviews: The case study and its findings were evaluated rigorously through interviews with domain experts.

It is important to note that the limited availability of prior research on applying outlier techniques in healthcare fraud detection makes this a practice-based issue. In such cases, the experiences and insights of

practitioners and the specific context play a crucial role in understanding and addressing the problem (Benbasat et al., 1987; Yin, 2011).

6.4.1 Metric Identification

From over a hundred metrics gathered from The FBI Federal Fraud News Reports (U.S. Federal Bureau of Investigation, 2013) and the National Association of Medical Fraud Control Units Fraud Reports spanning 2004–2012 (National Association of Medical Fraud Control Units, 2013), 13 specific metrics were chosen for the case study. These metrics were selected based on consultations with experts who evaluated their relevance to the dental domain and their potential effectiveness in detecting fraud.

The metrics were further categorized into groups based on the types of fraud they were most likely to reveal, with these categories and the associated data mining methods or outlier detection technologies outlined in Table 8.

To analyze the data, the selected metrics (or combinations of metrics) were visualized using scatter plots created in R (The R Foundation, 2015). This visualization helped illustrate the data distribution. Subsequently, various algorithms, cluster analyses, or linear models were employed to generate boxplots, which provided a graphical representation of the numerical data and highlighted any outliers.

Given that the dental domain tends to exhibit less variability than many other medical specialties, it was assumed that the metric scores relative to organizational size or claim submission volume would follow a normal distribution. On this basis, the outlier detection strategy was built around a Gaussian distribution of the data. Even though the data points did not adhere perfectly to this distribution, each metric was assigned specific outlier criteria, defined as a certain number of standard deviations away from the mean.

Outliers were identified on one tail of the distribution, at 1.96 standard deviations from the mean, capturing the upper 2.5% of data points. This approach aligns with the notion that overutilizing claimed resources often characterizes fraud. However, when the data did not follow a normal distribution, the threshold for outlier detection was adjusted to 2.33

standard deviations from the mean. This adjustment aimed to narrow the focus to the most extreme cases, which are more likely to indicate fraud.

Metric	Method	Outlier detection
• Reimbursement per beneficiary • Number of reimbursed claims over time	• Linear model outlier detection	• Trend deviation above threshold
• Number of reimbursed claims over time • Dollar amount of reimbursed claims over time	• Linear model outlier detection	• Deviating trend from peer group
• Proportion of weekend claims	• Univariate outlier detection	• Z-score above threshold
• Average number of reimbursed claims per beneficiary • Average amount reimbursed per beneficiary • Average number of reimbursed visits per beneficiary last 12 months • Amount of beneficiaries with a high number of yearly visits • Average number of reimbursed procedures per claim proportion to the number of reimbursed high-cost claims	• Multivariate outlier detection, cluster analysis	• Mahalanobis distance above the threshold, deviating cluster, deviation from nearest cluster
• Procedure code • High-cost procedure • Tooth code	• Box-plot outlier detection	• Peak deviation above threshold

Table 8 – Overview of metrics and the outlier techniques used.

6.4.2 Data Collection

Subsequently, a collection of dental claims was compiled to facilitate the experimentation with the selected metrics. In developing a prototype aimed at fraud analysis and visualization, detailed in Section 6.5, we ensured the assembly of a representative data set. This data set comprised Medicaid dental claims from a single state, spanning 11 months.

In collaboration with subject matter experts, specific criteria were established for the data set to mitigate the impact of external factors that could distort the analysis. These criteria ensured that:

- The data set encompassed all claims submitted within the specified time frame.
- All adjustments made to the submitted claims were included.
- There were no significant changes in the Medicaid State policy during the duration covered by the data set.

By adhering to these criteria, we aimed to maintain the integrity and reliability of the data, ensuring a solid foundation for the subsequent analysis.

6.4.3 Interviews with Experts

In the third step, the objective was to delve into the implications of the metric values and evaluate their practicality. To assess the utility of these metrics, interviews were conducted with professionals specializing in fraud detection. A semi-structured interview guideline was prepared, and each session was recorded to facilitate detailed analysis.

Opting for a semi-structured format allowed the experts to share their insights and reflect on the empirical results and experiential knowledge (Yin, 2011). Discussions revolved around the design of the metrics, the discerned patterns, and the implications of these findings, particularly in relation to potential fraud detection.

Experts from two distinct organizations affiliated with Medicaid were invited to participate. The interview session was unique in that both experts were present simultaneously, fostering a collaborative environment where they could openly discuss and debate the results in real time. Both participants were well-versed in national-level fraud prevention and possessed in-depth knowledge about the specific state under investigation.

6.5 The Fraud Detection Architecture

A data warehouse and analytics infrastructure were essential to streamline and facilitate analysis while presenting results in a coherent format. In response, we created an initial version of a fraud detection system. This system includes a cube for the multidimensional data model and a separate data store for the fraud metrics results. We then integrated these two sources to feed a fraud analysis and visualization tool, all under the

Centers for Medicaid and Medicare Services (CMS) data warehouse infrastructure specifically designed for this task. See Figure 28 for a visual representation of the architecture.

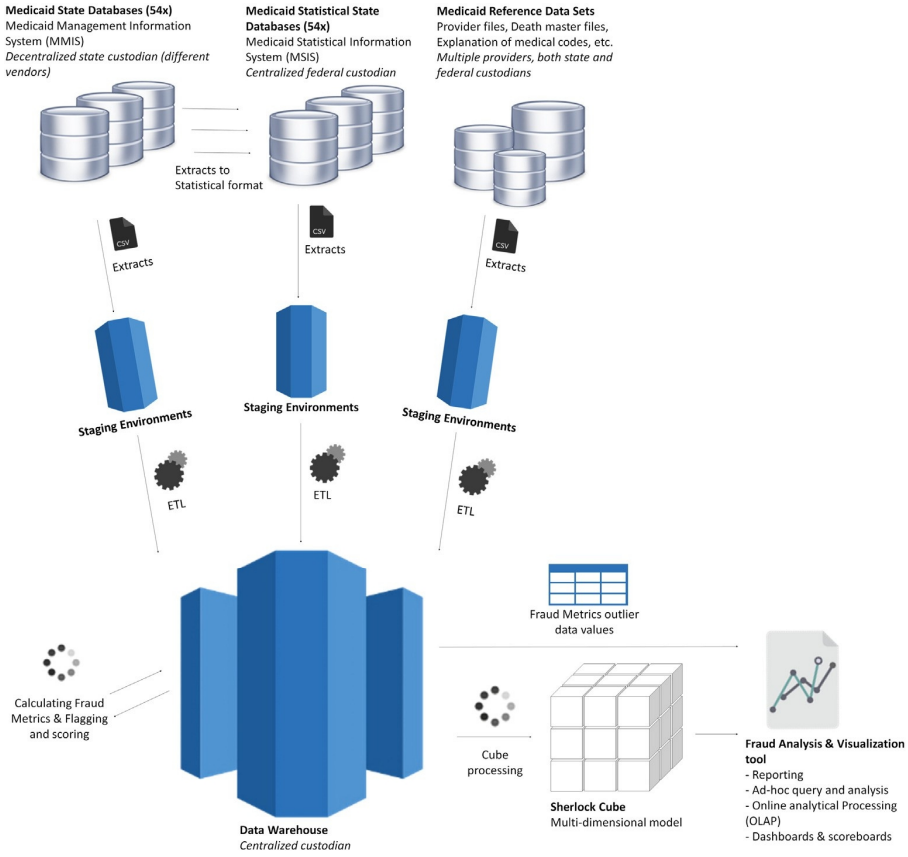


Figure 28 - Fraud Detection Architecture.

We loaded three distinct types of data files into the system:

- Provider claims in the specific format used by individual state Medicaid Management Information Systems.
- Federally determined statistical extracts for states, provided by the Medicaid Statistical Information System.
- Reference files from various states, CMS, and other governmental agencies. These files include vital information such as birth and death records, medical provider registrations, and criminal records.

These files underwent frequent distribution and parallel processing across multiple nodes before being consolidated in a single staging environment.

We took several crucial steps to maintain data integrity and completeness throughout this process. We processed and integrated adjustment claims with the original data. We systematically removed entries with inconsistencies, such as null values, zero-dollar payments, adjustments lacking corresponding original claims, and claims dated for future services. We also implemented procedures for duplicate detection, data reference checks, and format validation. We validated data files for completeness using metadata checks, including row counts and data structure validations. Upon successfully transforming the data to align with the data warehouse schema, we loaded it into the production environment. This environment allows fraud experts to conduct metric calculations and in-depth analyses.

Subsequently, we processed metric calculations, a task known for its intensive computational demands. To manage this, we stored the results in tables, ensuring they could be efficiently queried and integrated with the claims data from the multidimensional model.

We developed scripts to calculate and compare providers based on their metric scores to enhance our analytical capabilities. These scripts utilized analytical tools, including logical models, k-means algorithms, and boxplots. To guide these algorithms, we employed a parameter file, which allowed for the customization of data filters, setting outlier criteria, enabling write-back capabilities, and selecting visualization types for each experiment.

This meticulous process culminated in creating a robust fraud analysis and visualization environment. Through this platform, fraud experts are now equipped to conduct thorough investigations of flagged providers, drill down to the claim level, and scrutinize and compare outlier scores across different providers. Special attention and alerts can be proactively directed towards providers that have been flagged multiple times, enhancing the efficiency and effectiveness of fraud detection.

It is worth noting that while the current prototype presents fraud results in a static visual format and fraud experts primarily use traditional querying

tools for their inquiries, there is potential for significant advancement. Adopting interactive dashboards or advanced querying tools could further streamline the process, providing more targeted and efficient support for fraud experts, as Dilla and Raschke (2015) suggested.

6.6 Results

In this section, we present and apply literature-derived metrics, categorizing them by method and outlier detection technique, as shown in Table 8. We conducted 14 experiments, providing examples to illustrate identified fraudulent behavior through individual experiments. Additionally, we present an overview of the cumulative flagging results to assess the effectiveness of target selection using scoring. Finally, we provide a summary of the evaluation results from experts.

All experiments commenced with the same dataset, which underwent filtering through unique criteria at two different stages. The first stage of filtering, ensuring data integrity and completeness, occurs at the data loading stage and is detailed in Section 6.3.2. The second stage aims to prepare data for valid peer group analysis, excluding providers with a small number of claims, low reimbursement amounts, or few unique patients. Typically, the requirements for analysis were set at a minimum of $10,000 in reimbursed claims or at least ten unique beneficiaries per month. The resulting dataset comprised 369 providers, forming the basis for our analysis. Some experiments, such as the procedure code analysis, required a minimum annual service amount, excluding providers with low activity in these areas. This limitation enhanced the validity of the peer group analysis.

We employed multiple analysis techniques across the experiments, including variant, multivariate, time series, and boxplot analysis (refer to Table 8 for specifics). Each experiment also incorporated an outlier detection method, ranging from deviation from linear models, deviation clusters, single deviations from clusters, and trend deviations to peak deviations. These methods utilized both non-parametric and parametric (Gaussian mixture models) deviations.

Criteria were established in each experiment to define outliers. For example, in the linear model analysis, a deviation exceeding 2.33 standard

deviations from the general linear model classified a data point as an outlier. In the variant analysis, outliers were considered as groups, leading to the use of an outlying cluster algorithm. In the multivariate analysis using k-means clustering, outliers were defined based on deviation from their respective clusters. The experiments did not yield a significant number of outliers, preventing the performance of an outlying cluster analysis. Robust estimation procedures could mitigate the masking effect of outliers on sample means and deviations (Rousseeuw & van Zomeren, 1990). However, these were not applied in this study as the set of targeted outliers appeared to deviate sufficiently.

The approach advocates for a scoring mechanism to identify targets for fraud expert investigation. In this study, the scoring formula considered metric importance and historical data. Due to the limited dataset length, history was excluded from consideration. With only one full cycle completed, all metric flags were weighted equally to assess their impact and relevance without previous data to guide metric importance valuation. The cumulative flags from all experiments determined each provider's score.

The two-stage filtering process, multiple analysis techniques, and the scoring mechanism collectively contribute to identifying potentially fraudulent activities for further investigation by fraud experts.

6.6.1 Outliers Based on Linear Model

Figure 29 presents an outlier analysis identifying deviations from a simple linear model. This analysis plots the relationship between the total dollar amount reimbursed and the number of reimbursed claims for each provider. The red line represents the fitted general linear model (GLM) through the data points obtained using the linear model function from R, tailored for simple linear regression analysis. Notably, no offset was applied in the linear fitting, indicating no adjustment to the coefficient for corrective behavior. Additionally, the GLM did not account for NULL values, as these were removed in the earlier stages of data preparation. The blue lines indicate the boundaries set at 2.33 standard deviations from the linear model, identifying outliers that significantly deviate from the expected trend.

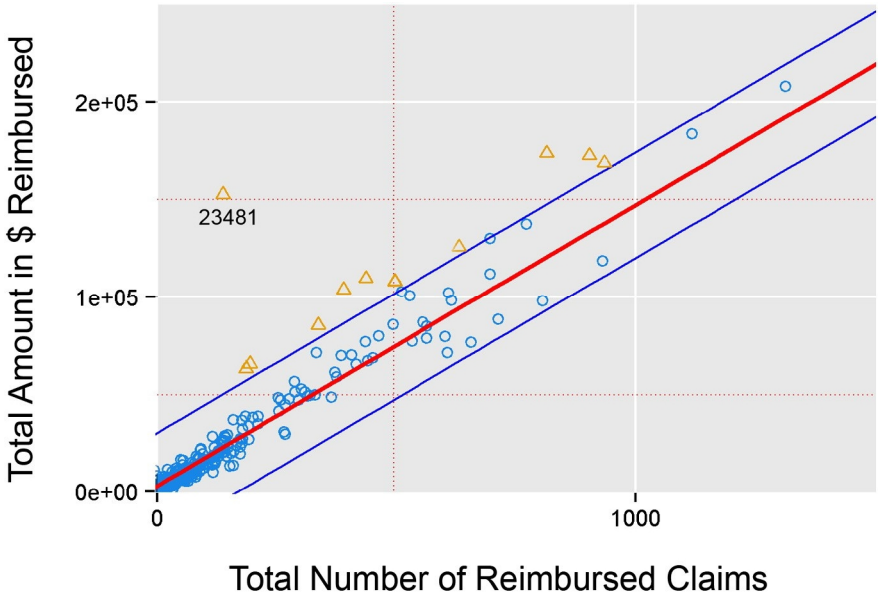


Figure 29 - Example Outliers on a Simple Linear Model.

Provider 23,481, marked in the top-left corner of the plot, demonstrates a significant deviation from the expected trend, thus drawing attention for further analysis. This provider submitted over 200 claims that month, with 30 deemed high-cost. Most of these high-cost claims were for complex, comprehensive orthodontic treatments (coded D8080, D8090, and D8999). Given that all dentists with a declared specialty were excluded from this study, this provider's submission of numerous specific high-cost procedures raised suspicions.

However, the fraud experts pointed out that there could be legitimate explanations for this behavior. For instance, provider enrollment registers might be outdated, or a provider's specialty might be misclassified as a non-specialty under Medicaid program regulations. When examining the flagging results, it was noted that this specific provider received six flags, leading the fraud experts to classify it as a case warranting a formal investigation. This example underscores the importance of expert evaluation in interpreting outlier analysis results, ensuring that anomalies are thoroughly investigated to distinguish between fraudulent and non-fraudulent behavior.

6.6.2 Boxplot Outlier Detection

The tooth code analysis compares providers based on the percentage of dental claims made for specific tooth codes. This analysis technique was inspired by a documented fraud case, where some dentists repeatedly claimed for the same set of procedures, merely altering patient IDs. This allowed them to maximize reimbursement with minimal effort. Providers engaged in fraud schemes, such as phantom billing, duplicate billing, or unbundling of claims, may become conspicuous if they do not sufficiently randomize the properties of their claims, leading to disproportionately high claims for specific tooth codes. Additionally, this analysis could uncover fraudulent practices such as recursive treatment on a tooth, where a dentist may fill a tooth, perform a correctional procedure, extract the tooth, and then implant a replacement. While these procedures may sometimes be justified due to medical reasons or misdiagnoses, their prevalence should be relatively low across the patient population.

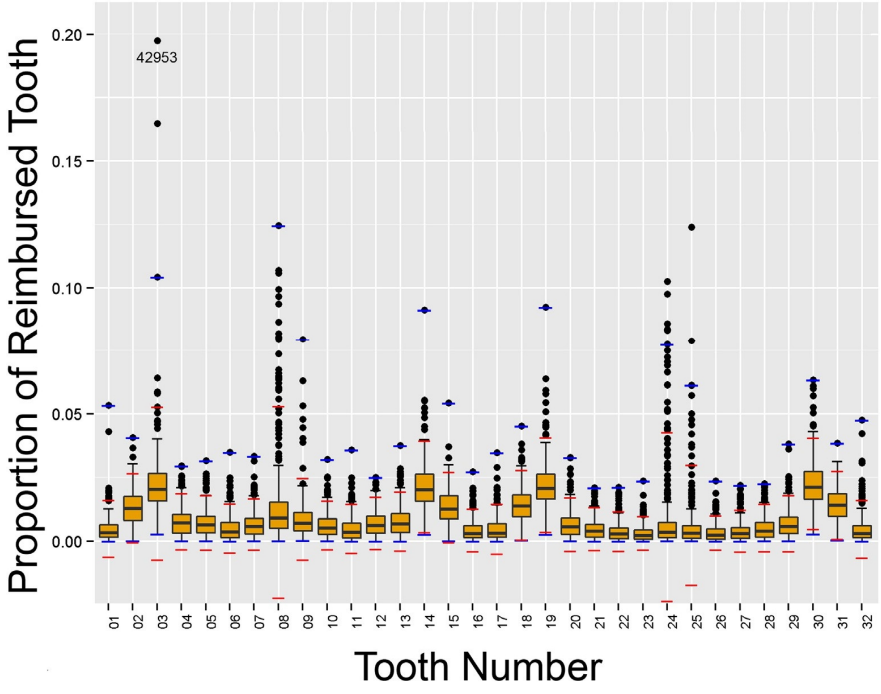


Figure 30 - Tooth Code Analysis (Adult Teeth)

Figure 30 illustrates this analysis through a series of boxplots, each representing a different tooth code. This analysis focuses exclusively on permanent adult teeth, excluding children's and supernumerary (extra) teeth. The teeth are numbered from the upper left to the upper right side of the mouth. Outliers, depicted as black dots, are identified as values exceeding the fourth quartile. However, since numerous providers have claims slightly above this quartile, the k-value in the boxplot formula, which determines the upper limit for outliers, was adjusted to increase the threshold for outlier detection. Typically, the k-value is set at 1.5, represented by the black whiskers in the plot. For this analysis, however, the k-value was increased to 12, creating a more stringent criterion for outliers, as shown by the blue whiskers extending above the boxplots.

$$Outliercriteria = Q_3 + k \cdot InterQuartileRange$$

In the analysis, provider 42,953 stands out for claiming over 140 procedures, nearly 20% of its total dental claims, under tooth code number 03. A detailed examination at the claim level revealed that these claims were distributed across multiple patients, generally with one or two instances of this procedure pattern per patient. Most of these procedures were coded as D0120, signifying a periodic oral evaluation for an established patient. This claim pattern persisted throughout the data collection period, suggesting a potential 'steal a little, all the time' fraud tactic. While this metric proved helpful in raising suspicions of fraudulent activity, it is noteworthy that this provider did not trigger any other flags in the various experiments conducted.

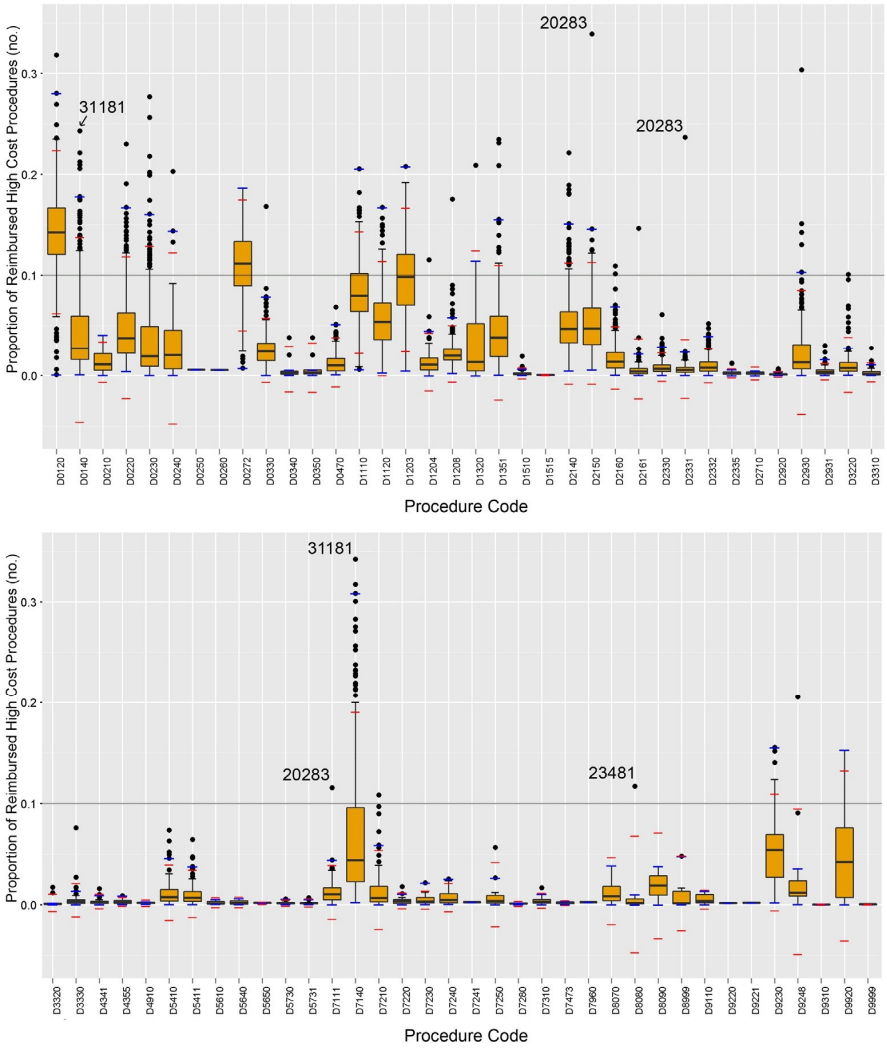


Figure 31 - Procedure Code Analysis

A similar boxplot analysis was applied to procedure codes associated with claims. Figure 31 displays a boxplot for each submitted procedure code. This analysis implemented an additional criterion, requiring a minimum of 300 claims per provider (each claim associated with a specific procedure code) to ensure sufficient data for reliable percentage comparisons. The same outlier detection formula used in the tooth code analysis was applied here, albeit with a necessary adjustment to the k-value. For this analysis,

the k-value was set to 3 to isolate the most extreme outliers above densely populated regions of data points. In Figure 31, provider 20,283 is highlighted as an anomaly; this provider excessively used three specific procedure codes: D2150 (Amalgam), D2331 (Resin-based composite), and D7111 (Extraction, coronal remnants). As a result of this pattern, the provider accumulated a total of five flags and was subsequently flagged for further investigation by the fraud experts.

Provider 38,606 also garnered attention for claiming over 40% of its procedures under the examination code D0140. A pattern emerged where many patients underwent multiple examinations in the months surrounding their tooth adjustments, with some patients receiving up to 15 examinations. In one case, a patient had a tooth extracted, underwent six examinations, and then had a second tooth extracted. While the sequence of claims is not inherently fraudulent, the frequency and repetition of such cases within a short timeframe raise suspicions. Despite these irregularities, provider 38,606 only received one flag in this analysis.

6.6.3 Outlier Detection Based on Peak Analysis

Figure 32 displays the claim submission patterns over time for two providers flagged in a peak analysis. This analysis was conducted to identify sudden and significant fluctuations in the number of claims submitted by providers every week. Specifically, outliers were defined as instances where a provider's weekly claim submissions doubled or halved compared to the previous week. These outliers are highlighted with thick black dots in the figure.

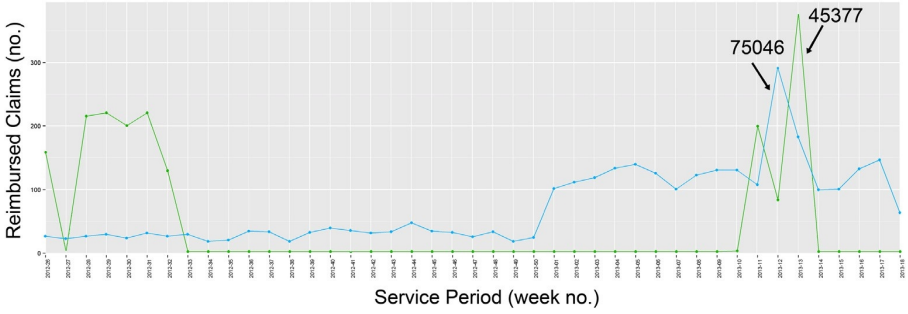


Figure 32 - Peak Analysis: Time Series with Outliers of Reimbursed Claims

Provider 45,377 exhibited a notable pattern, with no claims submitted for an extended period until week 10. Then, in week 13, there was a sharp increase to over 300 claims submitted. This change could be explained by the provider billing under multiple IDs, experiencing issues with their claim registration system, or, more plausibly, operating as a mobile dental practice. Ultimately, this provider received one flag in the analysis.

Provider 75,046 presents another intriguing case due to a substantial spike in claim submissions during week 12 of 2013, where the number of claims jumped from around 100 per week to almost 300. A detailed examination of the service code patterns within these claims heightened suspicions. A noticeable pattern emerged where many children received identical treatments on different teeth within the same week. The repetition of two specific treatment patterns was deemed worthy of further investigation. The first pattern involved a series of procedures typically performed on a child, including an oral examination, two bitewing films, two periapical films, prophylaxis, and a fluoride treatment. The second pattern mirrored the first but was designed for adults, adding three amalgam claims for each patient. The medical necessity of multiple films for each visit and the recurring use of three amalgams was considered unusual. As a result of these findings, provider 75,046 was flagged six times and flagged for a formal investigation by fraud experts.

6.6.4 Outlier Detection Based on Multivariate Clustering

Figure 33 illustrates the results of an experiment combining multivariate clustering and outlier detection to analyze healthcare provider behavior. The focus was on smaller providers, who typically exhibit more varied y-values. To account for this, multivariate clustering was applied using two attributes: one metric related to multivariate analysis (as outlined in Table 8) and the number of unique beneficiaries served by the provider.

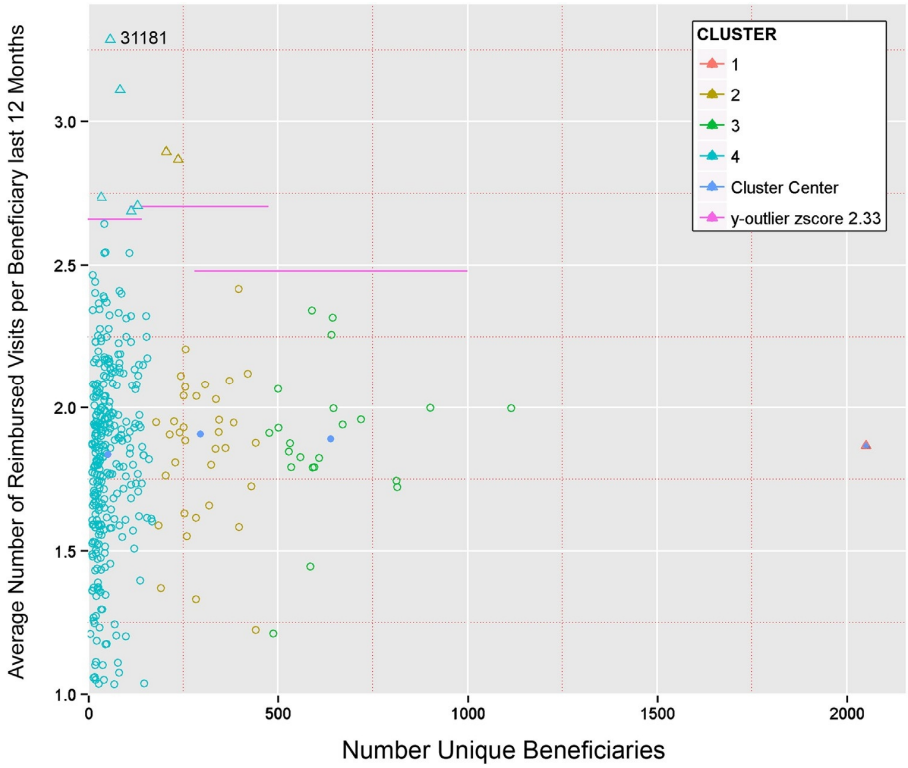


Figure 33 - Multivariate Clustering and Outlier Analysis

Before conducting outlier analysis based on the y-axis metric, clusters were formed to ensure that providers could be compared within groups of roughly equal size. The k-means algorithm, a straightforward and widely used unsupervised learning method, was employed to create these clusters around central points. To determine the optimal number of clusters, we looked for the "elbow" in a function plotting the sum of squared errors (SSE); the most pronounced bend was observed at four clusters. Notably, one of these clusters contained only a single, unusually large provider, which could not be compared to peers. Recognized as a significant entity, this provider necessitates a distinct approach to fraud analysis. Since it was placed in its own cluster, it received no flags in this analysis. In similar cases, alternatives might include excluding such large providers or reassigning them to a cluster of the next largest providers.

The pink line in Figure 33 denotes the threshold for outlier detection, set at 2.33 standard deviations above the mean of each cluster on the y-axis. Providers exceeding this value were identified as outliers and flagged accordingly.

Additionally, this methodology facilitated the analysis of recurring patient visits. A "visit" was defined as all claims submitted for a single patient within one day. Provider 31,181 received four flags and had an outlier average recurring visit rate of 3.29, significantly higher than the cluster mean of 1.84 visits per year. This was primarily attributable to a high frequency of follow-up oral evaluations for numerous patients. Furthermore, this provider predominantly submitted claims for tooth extractions, corroborated by a flag received for an excessive percentage of extraction codes in a separate procedure code analysis. All teeth appeared extracted for some patients, resulting in substantial insurance claims. While dental extractions are a common precursor to denture installation, frequent provision of dentures by a non-specialist dentist raises suspicions. Although this could be a legitimate specialty service, it is also a known Medicaid fraud scheme (U.S. Office Inspector General & Murrin, 2015). Therefore, experts recommend requesting documentation for multiple such treatments to ensure the validity of the claims.

6.6.5 Evaluation by Experts

Choosing a target percentage for investigation is a crucial step that should align with the available fraud expert resources and the allotted time for examination. While no standardized heuristics exist to determine the ideal target size, a 5% threshold was deemed a practical starting point for our process.

Table 9 outlines the distribution of flags assigned to providers during various experiments, categorizing them into two groups: those with zero to two flags and those with three or more flags.

The group with three or more flags represented approximately 5% of the providers, aligning with our predefined target. Ideally, all flagged cases would undergo review, but the sheer volume of cases rendered this impractical. Consequently, we scrutinized only a few exceptional cases from the zero to two flags group, specifically those exhibiting extreme

outliers, to ascertain if potential fraud could also be identified. It is important to note that due to the selective nature of this sample, no specific target success rate is established.

A. 352 of 369 providers received two or fewer flags, and a sample of extreme outliers was analyzed.			
Analyzed	**Flags received**	**Number of providers**	**Discussed in text**
Sample	0 flags	263	
	1 flag	71	42953, 38606, 45377
	2 flags	18	
Total		**352**	

B. 17 of 369 providers received three or more flags; all were analyzed.				
Analyzed	**Flags received**	**Number of providers**	**Reported**	**Discussed in text**
All	3 flags	8	4	
	4 flags	3	3	31181
	5 flags	2	2	20283
	6 flags	3	3	23481, 75046
	7 flags	1	0	
Total		**352**		

Table 9 - Flagging Results

Throughout the experiments, 369 providers were subject to flagging. Of these, 106 providers (28.7%) received at least one flag, 35 providers (9.5%) received more than two flags, and 17 providers (4.6%) received three or more flags. To assess the effectiveness of our approach, we conducted a detailed review of these 17 providers who received three or more flags.

Subject matter experts in healthcare fraud were consulted to analyze the results of our experiments, with a particular focus on the extreme outliers and the 17 providers flagged three or more times. Although some flagged instances could be justified by the nature of the services provided or the unique circumstances of the provider's operational environment, a significant portion of the findings—precisely 12 out of the 17 providers (or 71%)—were deemed worthy of a formal investigation. This conclusion was drawn based on the sufficiency of the evidence to meet the criteria for a

fraud expert to initiate an audit involving an in-depth examination of the providers' claims and a commitment of substantial investigative resources.

Conversely, the remaining five providers (or 29%) were determined to be misclassifications. The anomalies associated with these providers could be attributed to particular characteristics of their practice or were not deemed sufficiently compelling to warrant a formal investigation. While the analysis did reveal the potential for fraud detection among providers with only a single flag, there was a noticeable decline in the likelihood of uncovering fraud as the number of flags decreased.

The fraud experts acknowledged the utility of outlier detection in uncovering fraudulent activities, highlighting its potential advantages over costly periodic reviews. However, they also pointed out several limitations. Firstly, outlier detection technology is still in a nascent, experimental stage and has not yet proven its efficacy over the long term. Secondly, this method is inherently more complex than manual reviews, necessitating collaboration between technology and domain experts to devise appropriate metrics and interpret the results accurately. Thirdly, validating the effectiveness of outlier detection remains a challenge, as experts continue to rely on heuristics and industry-specific knowledge while exploring ways to enhance the fraud investigation process through technological means.

While outlier detection may not yet be a definitive method for fraud classification, it does offer valuable leads for further investigation. The experts suggested that technology should be viewed as a facilitator, enhancing interactive visual analytics and supporting the work of program integrity units in collaboration with legal authorities. Interactive visualizations enable investigators to navigate large datasets, manipulate data representations, filter transactions for more in-depth analysis, and, ultimately, increase the efficiency of fraud detection (Dilla & Raschke, 2015).

The experts highlighted boxplot analysis as a promising technique, noting its relative simplicity and ease of use for fraud experts, even with minimal guidance. The boxplot method allows for consistent application across

various metrics and provides a straightforward means of identifying outliers, making interpreting results less labor-intensive.

6.7 Discussion

Fraud detection within the U.S. medical insurance sector is a pressing issue with significant financial implications. The application of outlier detection has demonstrated its utility as a strategic approach to uncovering fraudulent activities, particularly in identifying potential fraud cases and serving as a valuable interactive tool for investigators.

In this study, extreme outliers were instrumental in highlighting irregular billing practices by providers, prompting experts to recommend comprehensive formal investigations. The analysis focusing on dental procedures and associated codes yielded the most promising results. Box plots emerged as a highly effective tool, uncovering numerous potential fraud cases and providing a straightforward, user-friendly data analysis and interpretation method. The findings suggest a clear correlation between the number of flags assigned to providers and the likelihood of fraudulent activity, underlining the effectiveness of this approach in pinpointing potential perpetrators of fraud. Nevertheless, to truly gauge the success of this method in selecting targets for investigation, long-term monitoring and subsequent evaluations based on confirmed fraud convictions are necessary. While this extended analysis was beyond the scope of the current study, it is a critical avenue for future research.

The study, however, is not without its limitations. The reliance on a small expert panel comprising only two individuals is a notable constraint. Additionally, variations in Medicaid program policies across different states may impact data completeness and accuracy, influencing the selection of metrics, thresholds, and detection methods. Although we anticipate that the findings are largely transferable to other health programs, with minimal adjustments, these factors should be considered when applying the study's results in different contexts. The study also highlights the need for careful consideration when choosing the size of the provider groups to target in relation to expected detection rates. While domain expertise and heuristics are invaluable at the initial stages of such investigations, there is potential for further research and development.

This study's focus on the dental domain, characterized by its relative homogeneity, presents an ideal scenario for applying outlier techniques. To enhance our understanding of the effectiveness of these methods, future research should explore their application in other medical domains, characterized by more complex billing structures.

A review of related literature reveals various data mining approaches applied to healthcare fraud detection, with varying degrees of success. While some studies report only a handful of identified cases (Major & Riedinger, 2002; Shan et al., 2008; Yamanishi et al., 2004), others boast two-thirds or higher detection rates (Ng et al., 2010; Ortega et al., 2006; Yang & Hwang, 2006). It is crucial to acknowledge that these results are influenced by numerous factors, including the definition of 'potential fraud' as opposed to confirmed cases. Nevertheless, there is a consensus on the value of data mining methods, such as outlier detection, for identifying and targeting fraudulent activities. By combining claims history with visualization tools and dashboards, outlier detection facilitates peer group analysis, enabling the swift identification of problematic providers and raising flags for further investigation.

6.8 Conclusions and Future Work

This chapter provides a practical case study for healthcare fraud detection, applying outlier detection to real Medicaid dental insurance data and involving two experts to assess the results. We outline an architectural design for identifying fraud in healthcare and introduce 14 pertinent metrics derived from fraud case reports and relevant literature. Utilizing these metrics, a series of experiments were conducted using outlier detection on a state-wide database containing actual dental healthcare claims from 369 providers. The analysis revealed significant patterns of potential fraud, which were subsequently discussed with fraud experts and illustrated in this paper.

Key lessons were learned about enhancing fraud prevention efforts:

- Substantial expertise in healthcare is crucial for developing analysis techniques and interpreting data mining results.
- Outlier detection proved to be an effective aid for fraud investigators in identifying potentially fraudulent activities. Of 369

primary dental providers analyzed, 17 (5%) were flagged for further scrutiny. Expert evaluation deemed 12 of these 17 providers (71%) as potentially fraudulent, meriting formal investigation.

- Visualizations and outlier detection can facilitate the identification of providers exhibiting anomalous and possibly fraudulent claim patterns, suggesting that this approach could be pivotal in creating a decision support tool to help investigators more efficiently target fraudulent providers.

The approach demonstrated in this research shows potential, especially when contrasted with previous success rates of around 10% (Major & Riedinger, 2002). The study lays the groundwork for future research, suggesting a need for a more detailed examination of specific outlier detection techniques suited to different types of healthcare fraud. Additionally, it calls for a broader evaluation of strategies and models for storing and preserving metadata, facilitating automated scoring, enhancing model adaptability, and allowing for data reconstruction.

In terms of long-term research goals, there should be a focus on pinpointing factors contributing to success and exploring supervised outlier detection methods. There is also a need to assess how well this methodology can be adapted to healthcare domains that are less uniform in nature to understand better the modifications required for outlier techniques when dealing with a variety of provider types.

This case study contributes to the existing body of knowledge, providing a thorough analysis with implications for future applications of outlier detection in healthcare and potentially related fields. It delves into the nuances of using this approach within the Medicaid dental context and highlights necessary considerations for applying these methods across other data landscapes. Ultimately, the research seeks to propel healthcare fraud detection and prevention advancements, supporting healthcare administrative agencies and law enforcement entities combating this pressing challenge.

7

Chapter 7: Design Principles for Fraud Detection in Complex, Multi-Stakeholder Systems

Chapter 7: Design Principles for Fraud Detection in Complex, Multi-Stakeholder Systems

7.1 Overview

The preceding chapters have centered on tackling fraud, waste, and abuse issues within the healthcare sector. I contend that the insights gained from addressing these challenges in healthcare can be extrapolated and applied to various other intricate domains. In this chapter, I put forth a set of specific design principles derived from valuable experiences in healthcare fraud detection and prevention. It is important to note that these principles are not presented as a comprehensive or optimal set of guidelines applicable to all domains. Instead, I propose that they offer a valuable perspective that could potentially be relevant and useful in many complex, multi-stakeholder environments.

Herein, I will outline these design principles and elucidate critical lessons learned from my involvement in Medicaid fraud detection. These will be substantiated with justifications and parallels drawn from published works in other related fields, reinforcing that these principles hold merit beyond the healthcare context and may be adaptable to various settings.

7.2 Design Principles

Design science has increasingly embraced design principles in characterizing the design process. Fu (2016) provides an extensive literature review and analysis of design principles in design research. It offers the following definition of a design principle.

Principle: A fundamental rule or law, derived inductively from extensive experience and/or empirical evidence, which provides design process guidance to increase the chance of reaching a successful solution.

This definition is aligned with the “action-centered guideline model” of Nowack (1997), where the design cycle is characterized by an “issue” addressed by an “action” which creates a “consequence” that can be

evaluated. Additionally, Fu's analysis builds on Greer's (2008) work that stresses imperative and action-centered grammar.

Turning to the domain of Information Systems (IS) research, Gregor (2020) introduces a framework for expressing design principles, encompassing four key elements: a) the aim, implementer, and user; b) the context in which the principle is applied; c) the mechanisms or actions undertaken; and d) the rationale underlying the principle. In alignment with this framework, this chapter presents a series of design principles articulated using the schema proposed by Gregor.

7.3 Design Principles for Fraud Detection in Complex, Multi-Stakeholder Systems

The design principles presented in this chapter are organized in relation to an adapted Knowledge Discovery from Data (KDD) (Fayyad et al., 1996) process representative of a typical operational fraud detection operation.

Figure 34 – Adapted KDD Fraud Detection Process

In this model,

1. the ongoing business and technical requirements for the system design are defined and constantly refined in **Business Context**,
2. **Data Collection** includes data selection and acquisition,
3. **Preparation** includes data pre-processing and transformations,
4. **Analysis** includes both human-led data mining and ongoing analysis processing operations of production analytics models,
5. **Findings** is the methodology for presenting the outputs of Analysis for action, and
6. **Feedback** includes feedback from the evaluation of Findings, the evaluation of data issues (i.e., quality, veracity, etc.), new data availability, and evolving business context inputs.

These phases provide context for the proposed design principles' use.

As Begoli and Horey (2012) discuss in their analysis of generalized design principles for knowledge discovery in big data, KDD is an interdisciplinary and evolving field, constantly guided by improvements in domain understanding, data, and available technologies, tools, and methodologies.

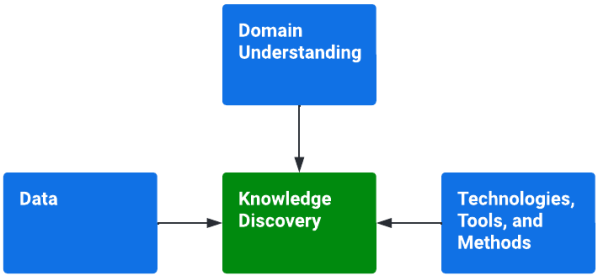


Figure 35 - Elements of the Knowledge Discovery Process, Adapted from Begoli & Horey (2012)

Further, Bachhety (2020) describes Intelligent Data Analysis (IDA) and the importance of enabling subject-matter expertise and domain understanding to drive the KDD process in a substantially complex domain.

KDD for fraud detection in a sufficiently complex, evolving domain is never a clean, linear process. The Fraud Detection Process Framework offered is merely a mechanism to categorize and provide context to the applicability of the proposed design principles, or, borrowing from the vocabulary of Nowack (1997), it classifies the types of "issues" that must be "actioned" to effect downstream "consequences."

The design principles offered are informed by preceding chapters, literature review, and industry experience developing operational systems to detect fraud, waste, and abuse in the healthcare domain. As discussed in Chapter 2, the US Medicaid healthcare system presents an extreme case of independent stakeholders with misaligned incentives, layers of principal-agent issues, data quality and veracity challenges, and impediments to actioning potential fraud, waste, and abuse. This perspective informs and colors the design principles previewed in Figure 36 and described in subsequent sections to address fraud detection in complex, multi-stakeholder systems.

Design Principle	ROI Delivery and Communication
Aim, implementer, and user	To allow anti-fraud practitioners (implementers) to facilitate ongoing program funding (aim) by program sponsors (enactors)
Context	In an operational program with the aim of detecting transactional fraud, waste, or abuse with discrete monetary value and with ongoing accountability and reporting requirements
Mechanism	Track and prioritize ongoing delivery and communication of return on investment (ROI), maximizing returns in each reporting period
Rationale	Because if program value can be communicated to sponsors, program investment and sustainability has a higher likelihood of being maintained.

Design Principle	Risk Signaling
Aim, implementer, and user	To reduce attempted fraudulent activity in a system (aim) by fraudulent actors (users) through signaling activity of program administrators (enactors)
Context	In an operational anti-fraud program
Mechanism	Enact signaling , such as publicly demonstrated enforcement actions, to discourage fraudulent actors
Rationale	To signal increased risk for fraudulent activity and reduce the appeal of being targeted in the first place

Design Principle	Subject Matter Expert Leadership
Aim, implementer, and user	To enable data scientists and engineers (enactors) to develop relevant and domain-responsive software and data artifacts (aim) useful to subject matter experts (users)
Context	In data collection for fraud detection
Mechanism	Work closely with subject matter experts to develop and iterate on target-state data models that include relevant domain features, processes, actors, and reference data; identify gaps in current data collection sufficiency or reliability to fulfill those models; and pursue opportunities to source additional reference or transactional data to improve observability
Rationale	Because subject matter experts are just that, "experts" in their domain, and can help guide technical developers in modeling the domain

Design Principle	Model Known Multiparty Fraud Schemes
Aim, implementer, and user	To enable data scientists and engineers (enactors) to develop relevant and domain-responsive software and data artifacts (aim) useful to subject matter experts (users)
Context	In data modeling for a domain that could include multiple actors collaborating on a fraud scheme
Mechanism	Model domain actor relationships for known multiparty fraud potentials
Rationale	Because this will inform the granularities of data models and analysis needed to identify these multiparty fraud schemes

Design Principle	Descriptively Model Actors and Relationships
Aim, implementer, and user	To enable data scientists and engineers (enactors) to develop relevant and domain-responsive software and data artifacts (aim) useful to subject matter experts (users)
Context	In data modeling for a domain that could include multiple actors collaborating on a fraud scheme
Mechanism	Descriptively model all potential actors, track actor features that could indicate relationships, such as locations or common transactional patterns, and leverage transaction data to build and maintain relationship graphs that describe both certain and probabilistic relationships
Rationale	Because this provides an understanding actors and potential relationships over time that can be useful in identifying single- and multi-party fraud schemes

Design Principle	Simple and Explainable Analytics
Aim, implementer, and user	To enable data scientists and analysts (enactors) to develop understandable and relevant software and data artifacts (aim) to non-technical audiences (users)
Context	In developing analytic models that must be presented and understood by lay audiences
Mechanism	Build using the simplest, most explainable analytics approaches that are effective
Rationale	Because this helps ensure results are as explainable as possible and not unduly paced by domain expert's understanding of more advanced data science methods

Design Principle	Ensemble Modeling
Aim, implementer, and user	To enable data scientists (enactors) to aggregate risk indicators across models, highlighting potential fraud targets (aim) for analysts and subject matter experts (users)
Context	In assessing fraud risk of system actors and actor networks
Mechanism	Employ ensemble modeling techniques to aggregate risk and highlight anomalous actors across models implemented over time and across varying granularities of actor groups with identified relationships
Rationale	Because aggregating model results can help enable the discovery of individual actors and networks of actors engaged in both known and unknown suspicious activity.

Design Principle	Target Known Knowns
Aim, implementer, and user	To enable data scientists (enactors) to build a baseline of actor participation in known fraud schemes and to enable targeting of said activity (aim) by analysts and subject matter experts (users)
Context	In assessing fraud risk of system actors and actor networks
Mechanism	Develop independent risk analysis models that target known fraud schemes at appropriately varied levels of actor, relationship, and transactional granularity, informed by known potentials for fraud
Rationale	Because building analytic models to address known fraud schemes can help enable the discovery of individual actors and networks of actors engaged in known suspicious activity

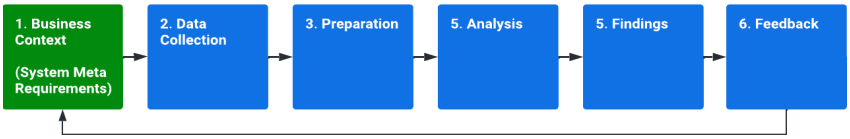
Design Principle	Audit-Ready Deliverables
Aim, implementer, and user	To enable an analytics team (enactor) to increase the likelihood of an audit recovery and minimize the amount of technical support (aim) for auditors (users)
Context	In a fraud detection program that refers cases to an audit process
Mechanism	Clearly define the methodology for presenting findings and delivering relevant case material to support target selection, audit execution, and case management
Rationale	Because audit teams are often not technical and need to fully understand the specific transactions, activity, and rationale for their audit target to maximize the likelihood of findings and recoveries.

Design Principle	Feedback and Improve
Aim, implementer, and user	To enable an anti-fraud program (implementer) to improve program performance through operational and actor-domain learnings (aim) by data scientists, data engineers, subject matter experts, and auditors (enactors)
Context	In an operational fraud detection program
Mechanism	Incorporate learnings from model performance, technology innovations, new data collection approaches, and stakeholder partnerships through continuous improvement
Rationale	Because audited model results can help improve existing models and external opportunities can help shape future insights, improving program performance and impact.

Figure 36 - Design Principles Overview

7.3.1 Define Business Context, Constraints, and Program Objectives

The **Business Context** phase sets and maintains the business requirements for the system design, defining the meta-requirements for the system and its processes. The policy and legal landscape inform the business context, the specifics of the business domain, and feedback from past analysis.



DP 1.1: ROI Delivery and Communication

Design Principle	ROI Delivery and Communication
Aim, implementer, and user	To allow anti-fraud practitioners (implementers) to facilitate ongoing program funding (aim) by program sponsors (enactors)
Context	In an operational program to detect transactional fraud, waste, or abuse with discrete monetary value and with ongoing accountability and reporting requirements
Mechanism	Track and prioritize ongoing delivery and communication of return on investment (ROI), maximizing returns in each reporting period
Rationale	Because if program value can be communicated to sponsors, program investment and sustainability has a higher likelihood of being maintained.

Program success is measured by results, and most programs maintain a cadence of reporting value to sponsors. In the work for CMS highlighted in past chapters, annual reporting was provided from the program to other parts of the agency, and those inputs were reported to the US Congress. Our CMS work closely tracked return on analytic models, audits, and state partnerships to demonstrate aggregate program return on investment in regular reporting activities to stakeholders. Externally, CMS provides an annual report detailing program activities, and a critical headline is always

program ROI. This is demonstrated on page one of CMS's FY2020 Medicare and Medicaid PI Report to Congress (RTC) (2020), in bold:

> *"In FY 2020, CMS's program integrity activities saved Medicare an estimated $11.8 billion and produced a return on investment (ROI) of $7.4 to 1."(CMS, 2020)*

Baesens (2015) discusses ROI development in anti-fraud programs, proposing a general methodology for calculating ROI. The methodology should be tailored to the use case and must be clear and defensible to withstand scrutiny. In evaluating ROI for fraud detection, the following general definition is followed:

$$ROI = (Returns - Costs) / Costs$$

Returns include:

- "Hard" impacts, such as recoveries, and
- "Soft" impacts, such as measured prevention, cost avoidance, and fraud deterrents that can be defended to sponsors.

Costs include:

- Direct program costs
- Indirect costs, such as
    - Impact to external customer stakeholders,
    - Customer support and retention,
    - Legal costs, and
    - Organizational program administration and review costs.
- Adverse impact of false positives, including
    - Wasted business partners' costs for justifying valid claims in a retroactive review,
    - Impact on customers and partners for stopping the delivery of needed goods or services in a prevention scenario, and

- Damage to brand.

Fraud detection must maintain a clear positive ROI that engenders confidence in the organization and does not impede organizational delivery goals. Higher ROI on an ongoing basis provides better program defensibility and begs the good investor's question of whether investing more will increase returns at a higher rate than the cost of capital. It should present the value of the program to stakeholders. "Soft" reputation and trust impacts of rooting out fraud and instilling confidence in the program are essential. They should be articulated, quantified, and cited in communication with sponsors.

DP 1.2 Risk Signaling

Design Principle	Risk Signaling
Aim, implementer, and user	To reduce attempted fraudulent activity in a system (aim) by fraudulent actors (users) through signaling activity of program administrators (enactors)
Context	In an operational anti-fraud program
Mechanism	Enact signaling, such as publicly demonstrated enforcement actions, to discourage fraudulent actors
Rationale	To signal increased risk for fraudulent activity and reduce the appeal of being targeted in the first place

Although it may not directly generate a "hard" return on investment (ROI) for the program, one of the primary and overarching objectives of fraud prevention initiatives is to dissuade fraudulent activities and actors. The intention is to capture and penalize fraudulent acts and create an unappealing environment for fraudsters. In the work conducted in support of CMS, as discussed in previous chapters, there was a strategic emphasis on striking a balance between recovering overpayments (resulting in hard returns) and collaborating with states to take visible legal actions. These legal actions served a dual purpose: a means of recovery and a public demonstration of the program's enforcement capabilities, designed to actively discourage fraud.

A case in point from our work with CMS involved a partnership between New Jersey and the federal government to take enforcement action against pharmacies that were billing both Medicare and Medicaid for the same prescriptions, effectively receiving double payments for a single drug. This clear violation led to settlement agreements, including an $8 million settlement with Omnicare, as reported by the Department of Justice (2017). In addition to recovering funds, these settlements were publicized through press releases by the U.S. Attorney's Office. This served as a celebration of the prosecution's success and a stark warning to potential fraudsters.

In analogous domains, Krawczyk (2009), building on Fudenberg and Maskin's (1986) folk theorem for repeated interactions in settings with numerous transient participants, concluded that it is beneficial for insurers to actively communicate their anti-fraud efforts. This communication demonstrates system vigilance and articulates the consequences of fraudulent behavior, aiming to deter dishonest practices. To operationalize this concept, Dionne (2009) formulated a model to optimize identifying and auditing potential fraud cases based on specific indicators. This model was empirically tested using data from a large European insurance provider. Intriguingly, the findings suggested that, in some instances, an optimal investigative strategy might involve audits that yield a negative hard ROI. This counterintuitive approach is justified by the deterrent effect created through the visible and active signaling of enforcement measures.

7.3.2 Collect Sufficient Data Reliably

Data Collection includes data selection and acquisition, including definition of features, data sources, and reliability considerations. Here, the desired business domain features are defined and cross-walked with the potential sources' veracity, velocity, and cost characteristics to optimize the data collection strategy.

DP 2.1 Subject Matter Expert Leadership

Design Principle	Subject Matter Expert Leadership
Aim, implementer, and user	To enable data scientists and engineers (enactors) to develop relevant and domain-responsive software and data artifacts (aim) useful to subject matter experts (users)
Context	In data collection for fraud detection
Mechanism	Work closely with subject matter experts to develop and iterate on target-state data models that include relevant domain features, processes, actors, and reference data; identify gaps in current data collection sufficiency or reliability to fulfill those models; and pursue opportunities to source additional reference or transactional data to improve observability
Rationale	Because subject matter experts are just that, "experts" in their domain, and can help guide technical developers in modeling the domain

In our work with Medicaid, significant reference data from CMS and third parties was sourced at the direction of subject matter experts to provide context for analysis and better represent medical sub-domains, extending the core data models described in Chapters 5 and 6. Examples include:

- Provider data was sourced from the CMS National Plan and Provider Enrolment System (NPPES), national and state exclusion lists, and directly from state provider databases to supplement claims information.
- CPT and HCPCS codes, used by healthcare providers to bill for services and supplies, were added to the model. CPT codes are published by the American Medical Association (AMA) and are used to identify medical services and procedures performed by physicians and other healthcare professionals, divided into six sections: evaluation and management (E&M), anesthesiology, surgery, medicine, radiology, pathology, and laboratory. HCPCS codes are published by CMS and are used to identify medical

services and supplies not covered by CPT codes, such as ambulance services, durable medical equipment, and prosthetics.

- Kaiser Family Foundation (KFF) reference data was added to provide national and regional context to health insurance coverage, healthcare costs, and access to care across the US. An independent non-profit that analyzes healthcare issues, KFF's data is regularly updated and based on various sources, including federal and state government data, surveys, and other research.

Subject matter experts were able to guide the development of information models to represent the healthcare domain properly and to source reference data sets that characterize various system activities, what "good" looks like, and relationships between multiple entities, services, diagnoses, and outcomes. Examples abound in the healthcare domain in general and, specifically, in combating healthcare fraud. J. M. Johnson and Khoshgoftaar (2022) demonstrate the usefulness of CMS's Medicare Part B "Summary by Provider" (SbP) and "Summary by Provider and Service" (SbPS) data sets in providing additional feature context to provider claim behavior. Hancock and Khoshgoftaar (2020b) demonstrate the significant impact of adding features from referential data to bring context to claims in CatBoost and XGBoost classification.

Data collection sufficiency in fraud detection is akin to complex system observability. Significant work in complex systems observability has been published, including Holmström (1979) and Y.-Y. Liu (2013).

"A quantitative description of a complex system is inherently limited by our ability to estimate the system's internal state from experimentally accessible outputs. A system is called observable if we can reconstruct the system's complete internal state from its outputs." (Y.-Y. Liu et al., 2013)

Fraud is committed by people and institutions that intend to deceive. Modeling those entities and understanding their behaviors beyond the context of a single transaction is critical to characterizing and classifying

what “fraudsters” can look like. In R. Bauder’s (2017) literature review on algorithmic methods to analyze or detect healthcare claims upcoding, he suggests,

> *“…in-depth data integration with publicly available big data sources, beyond those summarized in the reviewed literature, can also add to the meaningful detection of this type of fraud by including more relevant information and patterns aiding machine learning techniques.” (R. Bauder et al., 2017)*

Targeting new data sources unavailable today to claims processors, Matloob and Khan (2019) analyzed patients, providers (doctors, hospitals, and pharmacies), and services, using rich data from operational healthcare systems (instead of claims data) and applying clustering methodologies and outlier detection. With more detailed signal data, many anomalies were identified within and across the modeled entities that would not have been apparent in claims alone.

Kapadiya (2022) proposes adding patient health telemetry streaming from wearable devices, such as smart glasses, blood pressure monitors, fitness bands, and “smart shoes,” sending this data to health insurers to improve provider fraud detection modeling in exchange for insurer compensation to the patient. Developing a path for better patient telemetry data helps bypass some of the information asymmetry and data veracity challenges at the heart of fraud detection today.

Mavlanova (2012) evaluates online retailer signals as a method of discriminating between low- and high-quality sellers, developing a three-dimensional framework for relevant signals in e-commerce. One takeaway from applying this in the online pharmacy space is that “low-quality pharmacies try to avoid signals that are easily verifiable. On the other hand, high-quality pharmacies do not refrain from displaying signals that are easily verifiable as they are likely to be true.” Furthermore, “sellers that invest in high-cost signals are likely to display easy-to-verify signals. These findings are important as they show that signals are not used in isolation

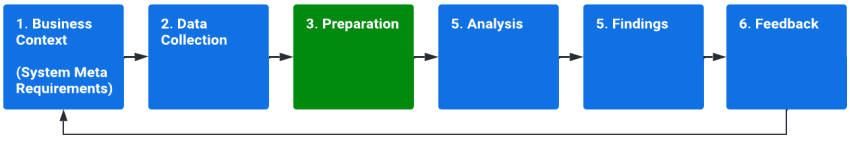
but clustered into groups with high-cost and easy-to-verify signals forming one, and low-cost and difficult-to-verify signals forming a second group."

Similar models could be built across other domains and inform the types of signaling requirements that could be implemented to reduce information asymmetry and increase risk profiling accuracy. For example, Hampshire (2017) explores applying signaling theory to evaluate the trustworthiness of healthcare providers in less regulated nations where information quality and availability are weak. The signals needed will go beyond the transaction and the domain to provide context on the actors themselves.

"…we need to work with different kinds of data and models, challenging and traversing standard disciplinary boundaries." (Hampshire et al., 2017)

7.3.3 Prepare Data to Represent the Domain's Reality

Preparation includes data pre-processing and transformations that make using the data more straightforward, accurate, and repeatable. With data spanning sources, addressing formatting issues, joins, authoritative source to feature mapping, and other transformations can help disparate data sets come together to represent ground truth better.



DP 3.1 Model Known Multiparty Fraud Schemes

Design Principle	Model Known Multiparty Fraud Schemes
Aim, implementer, and user	To enable data scientists and engineers (enactors) to develop relevant and domain-responsive software and data artifacts (aim) useful to subject matter experts (users)
Context	In data modeling for a domain that could include multiple actors collaborating on a fraud scheme
Mechanism	Model domain actor relationships for known multiparty fraud potentials
Rationale	Because this will inform the granularities of data models and analysis needed to identify these multiparty fraud schemes

Domain actor relationships and known potentials for multiparty fraud will inform the granularities of data models and analysis needed to identify these multiparty fraud schemes. As demonstrated in Chapter 5, network analysis techniques can be used to create a graph of the relationships between actors. This graph can be used to identify key players, potential collaboration patterns, and hidden connections among actors. In healthcare fraud, this includes evaluating what "normal" looks like at a point in time and over time at various granularities, including:

1. Individual Transactions
2. Individual Episode of Care Transaction Patterns (linked care transactions of one patient, potentially across providers)
3. Patient
4. Patient within a Cohort
5. Patient Episodes of Care over Time
6. Provider
7. Provider within a Cohort
8. Provider Network Relationships
9. Provider Evolution over Time

In addition to network analysis, other techniques, such as community detection and link prediction algorithms, can be used to identify potential

fraud schemes. These techniques can help identify groups of actors likely to be involved in fraudulent activities and can help identify potential new members of a fraud scheme.

Building on the CMS Dental approach presented in Chapter 6, Kumaraswamy, Markey, and Barner (2022) evaluated feature selection in pharmacy claims, analyzing 176 facets and distilling 15 features representing 85% of claim variance. Addressing known actor relationships in various potential fraud schemes, "A set of features were engineered following a logical inference of interactions between potential fraudulent actors" (Kumaraswamy et al., 2022). The work provides an analytical framework for converting prescription claims to features to fraud indicators, starting by modeling the domain actor relationships and known potentials for multiparty fraud.

In other published examples:

- Matloob (2022) applies sequence mining at a specialty, or sub-domain, level to determine normal and anomalous patient service sequences. These rules were informed by data but guided by medical experts in determining "frequent medical behaviors." Anomalous sequences, or episode of care patterns, can add to risk scoring or trigger audit activities.
- Ali (2022) recommends leveraging tools such as Word2Vec, Doc2Vec, or BERT to transform text data, such as medical codes and sequences, in this case, into vectors of features.
- Rayan (2019) presents models developed and used to evaluate claims, including patient claim experience, admitted hospital experience, ailment group analysis, policy riskiness, and demographic analysis.
- Verma (2017) demonstrates positive results from clustering and outlier analysis, evaluating period of care and disease-based patterns of care as critical discriminators.
- Rawte and Anuradha (2015) present a hybrid approach combining supervised (SVM classification) and unsupervised (Evolving Clustering Method, ECM) to provide responsiveness and adaptability to incoming data. Specifically, ECM is used to continuously adapt clusters that could represent new disease

modalities based on incoming data. In contrast, SVM uses this cluster affinity and other claim features, such as date, to classify appropriate claims as fraudulent, such as duplicate billings. This layered approach demonstrates how ongoing analysis can develop and maintain features that add context to claims analysis.

- Zhao (2019) proposes a methodology for developing and analyzing a "Dynamic Heterogeneous Information Network" graph, modeling the relationships between patients, providers, hospitals, conditions, and treatments. This promising approach could potentially be enhanced through J. M. Johnson & Khoshgoftaar's (2020) HCPCS2Vec methods and additional source data that improves the veracity of graph node data.

These examples collectively underline the importance of a nuanced approach to data analysis in uncovering healthcare fraud, emphasizing the need for a deep understanding of domain actor relationships and the various granularities at which analysis can be conducted.

DP 3.2 Descriptively Model Actors and Relationships

Design Principle	Descriptively Model Actors and Relationships
Aim, implementer, and user	To enable data scientists and engineers (enactors) to develop relevant and domain-responsive software and data artifacts (aim) useful to subject matter experts (users)
Context	In data modeling for a domain that could include multiple actors collaborating on a fraud scheme
Mechanism	Descriptively model all potential actors, track actor features that could indicate relationships, such as locations or common transactional patterns, and leverage transaction data to build and maintain relationship graphs that describe both certain and probabilistic relationships
Rationale	Because this provides an understanding actors and potential relationships over time that can be useful in identifying single- and multi-party fraud schemes

Transaction data is a powerful tool for building and maintaining relationship graphs, which help depict definite and potential connections between various actors. These graphs are insightful, illuminating how actors are interlinked and how these connections evolve over time.

Various graph analytics techniques can be employed to analyze these graphs and glean valuable insights, such as network analysis, community detection, and link prediction algorithms. These methods work together to both create and sustain the relationship graph.

Take, for instance, the case of healthcare, where multiple instances of patient care involving the same group of physicians could reveal a network of relationships between these doctors. It is crucial to note that such a relationship does not inherently imply wrongdoing. Instead, it represents "new data" or a newfound link. By leveraging graph analytics, we can dissect these links to distinguish between beneficial collaborations and potential instances of multiparty fraud.

In published examples:

- Jing (2019) proposes a graph-based credit card fraud detection framework using GraphSAGE on node classification. This approach offers promise in the healthcare fraud domain as additional reference datasets and probabilistic relationships discerned from claims patterns are added to provide context to claims data.
- Fursov (2022) demonstrates an approach to transform relational claims data into a graph, embedding object descriptions in vectors that belong in the same dimensionality as the graph nodes.
- Matloob (2020) demonstrates the usefulness of using time-series claims data to develop sequences of care that represent normal and abnormal behavior.
- S. Chen and Gangopadhyay (2013) apply spectral analysis to a two-mode network to detect communities and potential collusion between primary care providers and specialists. This approach could be extended to additional actors as those relationships are identified and added to the graph.
- R. Bauder (2017) suggests the exploration of "network (graph) analysis to create labeled data as well as methods to better

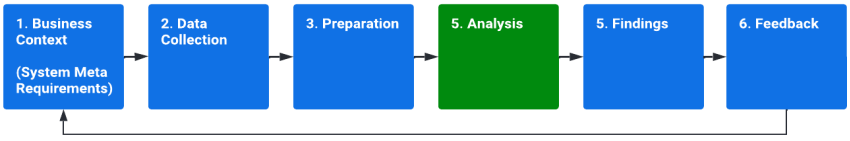
understand interactions between providers, especially with many integrated data sources, via referral analysis to mine any additional patterns."

- J. M. Johnson and Khoshgoftaar (2020) offer a graph vector development and evaluation method using Healthcare Common Procedure Coding System (HCPCS) codes embedded in claims. Word2Vec models are employed to derive semantic relationships between HCPCS codes, providing better context than traditional one-hot vector development with claims data alone by correlating like and related procedures.
- Haque and Tozal (2022) demonstrate a modeling approach to translate diagnosis and HCPCS codes into Mixtures of Clinical Codes (MCC), providing improved context to claim validity. These approaches to improving the information gained from simple codes are promising to enhance downstream clustering and outlier identification.

Transaction data, when utilized effectively through graph analytics, becomes a potent tool for unraveling and understanding the complex web of relationships among different actors, ultimately aiding in identifying both positive collaborations and potentially fraudulent activities.

7.3.4 Analyze, Guided by SMEs and the Specifics of the Domain

Analysis includes both new, human-led efforts and operational execution of production analytics models. This phase operates on incoming, prepared data and provides either direct findings or updated risk scoring based on new, incoming data.



DP 4.1 Simple and Explainable Analytics

Design Principle	Simple and Explainable Analytics
Aim, implementer, and user	To enable data scientists and analysts (enactors) to develop understandable and relevant software and data artifacts (aim) to non-technical audiences (users)
Context	In developing analytic models that must be presented and understood by lay audiences
Mechanism	Build using the simplest, most explainable analytics approaches that are effective
Rationale	Because this helps ensure results are as explainable as possible and not unduly paced by domain experts' understanding of more advanced data science methods

In the healthcare data mining process, it is crucial for subject matter expertise to take a central role, complemented by straightforward analytics methods that prove effective. Subject matter experts bring a wealth of domain-specific knowledge, enabling them to pinpoint pertinent data and formulate critical questions relevant to the context. Their insights are instrumental in steering the data mining process, ensuring the results are relevant and meaningful.

Throughout my work in healthcare fraud detection, the collaboration with subject matter experts – including physicians, policy specialists, and auditors – proved indispensable in achieving practical outcomes. Data scientists, on their own, can hastily draw conclusions from legitimate anomalies, subpar data quality, or variations in policy across different states. While they can apply clustering and other analytical techniques, distinguishing between "good" and "bad" outcomes necessitates the expertise of subject matter experts. Through a collaborative effort, data scientists and subject matter experts can iteratively develop and test fraud detection strategies, ultimately leading to actionable audit targets and substantial recoveries.

"In order for data science to flourish as a field, rather than to drown in the flood of popular attention, we must think beyond the algorithms, techniques, and tools in common use. We must think about the core principles and concepts that underlie the techniques, and also the systematic thinking that fosters success in data-driven decision making." (Provost & Fawcett, 2013)

Provost and Fawcett (2013) emphasize the importance of broadening our perspective beyond the technical means to a deeper understanding of the underlying principles and concepts. Subject matter experts are central to guiding data science activities to successful outcomes.

It is beneficial to prioritize simple yet effective analytical methods to encourage this productive collaborative partnership in the data mining process. Opting for basic techniques over more complex data science methods ensures domain experts can easily comprehend and interpret the results. This approach employs fundamental statistical techniques such as descriptive statistics, correlation analysis, and simple visualization methods. These techniques offer clarity and ease of interpretation and deliver valuable insights while reducing the risk of overcomplicating the results or fitting the model too closely to the data. By adopting these simple analytics methods, subject matter experts can contribute critical insights within their areas of expertise and confidently articulate and validate their findings.

Subject matter experts should be at the forefront of the healthcare data mining process, with their work augmented by these straightforward analytical methods to ensure effectiveness. These experts possess extensive field knowledge, enabling them to pinpoint the relevant data and formulate the crucial questions that need addressing within healthcare delivery. Their expertise is vital for navigating the data mining process and ensuring the results are pertinent and meaningful.

Kumaraswamy, Markey, and Ekin (2022) emphasize the importance of simplicity and transparency in algorithms used in healthcare fraud

detection. They argue, "Complex algorithms are difficult for the downstream examiner's team to understand and use. In a healthcare fraud business workflow, it is very important that the methods used in each step along the way are transparent and easy to comprehend." Therefore, algorithms should be only as complex as necessary and must be interpretable.

Adopting an approach led by subject matter experts and characterized by algorithmic simplicity enhances the ability to produce both interpretable and justifiable results. This approach also facilitates informed decision-making and the implementation of appropriate actions. In the CMS work discussed in previous chapters, the most effective audits were those based on unambiguous, simple algorithms. Identifying and auditing duplicate billings, upcoding, and unnecessary procedures and equipment that lack supporting diagnoses were relatively straightforward tasks, resulting in a high return on audits.

Panigrahi (2011) echoes this sentiment in the context of financial fraud detection, advocating for a process that leverages the expertise of auditors and simple analytic tools and techniques rather than focusing solely on advanced analytical models. He asserts, "…although many advanced techniques are available in the literature and implemented in software, simple techniques are useful for forensic auditors in many situations."

Navigating this balance is crucial in fraud detection. Data scientists should stay informed about the latest and most advanced algorithms and techniques. However, these advanced techniques must not become an obstacle for less technical users in making data-driven decisions and fulfilling the mission to combat fraud.

DP 4.2 Ensemble Modeling

Design Principle	Ensemble Modeling
Aim, implementer, and user	To enable data scientists (enactors) to aggregate risk indicators across models, highlighting potential fraud targets (aim) for analysts and subject matter experts (users)
Context	In assessing fraud risk of system actors and actor networks
Mechanism	Employ ensemble modeling techniques to aggregate risk and highlight anomalous actors across models implemented over time and across varying granularities of actor groups with identified relationships
Rationale	Because aggregating model results can help enable the discovery of individual actors and networks of actors engaged in both known and unknown suspicious activity.

An ensemble model enhances predictive performance by combining multiple sub-model forecasts to produce a more accurate and robust outcome. This approach is particularly beneficial in multi-stakeholder systems, where it supports detailed and varied risk analyses across different types of participants.

For instance, an ensemble model can integrate the results from various risk models, each tailored to assess specific groups such as patients, healthcare providers, or the larger organizations they are part of. Each sub-model operates independently, generating predictions based on its unique criteria and data relevant to its target group. The ensemble model then consolidates these individual forecasts, creating a comprehensive and multi-faceted risk assessment.

The ensemble model ensures a more accurate and reliable overall risk analysis by aggregating predictions from different sources. It considers the complexity and diversity of the healthcare ecosystem, providing a nuanced understanding of risk across various levels of actors. Employing an ensemble model in multi-stakeholder systems like healthcare allows for a

more detailed and comprehensive approach to risk analysis. It leverages the strengths of individual models tailored to specific groups, resulting in a robust and well-rounded risk assessment.

Skillicorn (2009) suggests the need for ensemble models and ensemble-like predictors to detect fraud in adversarial systems to counteract actor manipulations, as the ensemble of models builds predictions from different lenses spanning large data sets, improving confidence in the overall ensemble's prediction.

Ali (2022) states that "ensemble methods that take advantage of multiple algorithms to classify samples is a rising trend in the field."

M. E. Johnson and Nagarur (2016) demonstrate the usefulness of a multi-stage approach to risk analysis on claims, evaluating providers against their peers, claim parameters against patient populations, and claim amounts vs. expectations before aggregating these deltas and potential recoveries as weights for risk scoring to guide the audit process.

Anbarasi and Dhivya (2017) highlight the challenges of combining retrospective and proactive analysis. The proposed approach implements graph data modeling in a "policy verification module" preprocessing step and an outlier detection module that operates on the graph to further clean and filter the data, compute metrics, compare actors by metrics, and flag outliers. This continuous process updates the risk scoring of providers in the methodology.

DP 4.3 Target Known Knowns

Design Principle	Target Known Knowns
Aim, implementer, and user	To enable data scientists (enactors) to build a baseline of actor participation in known fraud schemes and to enable targeting of said activity (aim) by analysts and subject matter experts (users)
Context	In assessing fraud risk of system actors and actor networks
Mechanism	Develop independent risk analysis models that target known fraud schemes at appropriately varied levels of actor, relationship, and transactional granularity, informed by known potentials for fraud
Rationale	Because building analytic models to address known fraud schemes can help enable the discovery of individual actors and networks of actors engaged in known suspicious activity

Building upon DP 3.1, multiple analytics approaches can be targeted at various levels of data granularity. Prior chapters describe the development of multiparty fraud relationship models, the effectiveness of evaluating provider claim patterns vs. cohorts and inferring multiparty episode of care patterns across patients. Analytic models can and should target specific levels of actor and transactional granularity, enabling ongoing detection of known fraud schemes and risk flagging that can be further utilized in ensemble approaches, as described in DP 4.2.

Potentially as simple as “when there is smoke, there is likely fire,” throughout our work with CMS, we were able to target known knowns – simple schemes with clear patterns. While these models produced some direct, auditable results, they offered significant insight into providers and patients with increased risk. Audits of these providers often uncovered inappropriate activities outside of the original “known knowns” that triggered the audits.

Luan (2019) demonstrates the effectiveness of modeling relationships between doctors and drugs prescribed as a clustering and outlier detection mechanism. This paper confirms and references the approach from the Medicaid dental domain work from Chapter 6 in a different medical domain.

Sun and Yan (2019) propose methodologies for person similarity calculation and abnormal group mining, resulting in normal vs. suspicious group scoring. The model was evaluated using 40M records spanning 10k patients and improved on L-SVM classification, DILOF anomaly detection, BP-Growth pattern mining, and Abnormal Growth methods.

Liang (2019) presents an approach to evaluating potential collusion in healthcare network participants based on device utilization in China. This approach could have parallel applications in technical interactions with providers and patients with healthcare systems, as well as modeling medical billers akin to the "device" concept. Unfortunately, much of this system and "hidden" participant information is currently unavailable to claims processing and would need to be studied to evaluate collection methodologies and interactions with privacy requirements.

Sun and Li (2019) highlight a graph-based approach to clustering inpatient episodes of care and patients by demographics and then evaluating for similarities of similar patients to claimed patterns of care. Graphs can represent patterns of care much more directly and performantly than evaluating flat relational data, improving the efficacy of overall risk modeling.

J. Zhang (2022) demonstrates a Graph Neural Network (GNN) based methodology for evaluating the graph of transaction and actor relationships. Yoo (2022) and Wang (2022) demonstrate the efficacy of a graph sample and aggregate (GraphSAGE) based GNN in Medicare fraud detection. These types of approaches are needed to analyze the complex web of relationships in healthcare data and uncover potential multiparty fraud scenarios.

W. Zhang (2022) demonstrates a graph modeling and analysis approach to uncovering multiparty prescription fraud across pharmacies, providers, and patients.

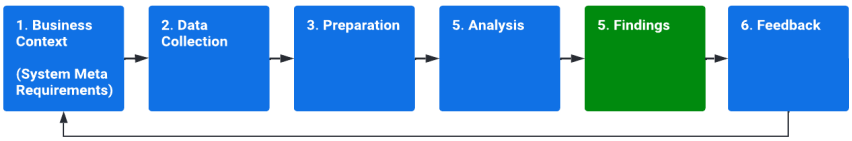
Yao (2021) proposes and demonstrates the efficacy of an improved bootstrap aggregation (Bagging) algorithm in detecting Medicare fraud. Bagging (bootstrap aggregation) algorithm to detect Medicare fraud. The weighted threshold method, WTBagging, improves on a traditional Bagging model, basing results on a weighted ensemble approach. Ensemble approaches are needed to effectively aggregate risk scoring across models to identify fraudulent transactions and actors.

Sadiq (2017) demonstrates an anomaly detection approach based on the Patient Rule Induction Method (PRIM) to flag physicians behaving abnormally. Results showed marked improvement in identifying risky providers more likely to commit fraud.

Settipalli (2022) presents the concept of "Drift Analysis in Decomposed Healthcare Claims (DADHC)" to evaluate and compensate for sudden or gradual shifts in a provider's claims behavior that seasonality, pandemics, or shifts in standards of care could explain. The study evaluates various approaches to windowing and proposes a topological clustering approach. Patterns of care change over time, and clustering models must consider this to minimize false positives.

7.3.5 Present Actionable Findings.

Findings is the methodology for presenting actionable analysis outputs to human and machine actors.



DP 5.1 Audit-Ready Deliverables

Design Principle	Audit-Ready Deliverables
Aim, implementer, and user	To enable an analytics team (enactor) to increase the likelihood of an audit recovery and minimize the amount of technical support (aim) for auditors (users)
Context	In a fraud detection program that refers cases to an audit process
Mechanism	Clearly define the methodology for presenting findings and delivering relevant case material to support target selection, audit execution, and case management
Rationale	Because audit teams are often not technical and need to fully understand the specific transactions, activity, and rationale for their audit target to maximize the likelihood of findings and recoveries.

Auditors require explicit guidelines and a record of any deviations from these standards to validate their audit findings and confirm instances of overpayments. Establishing a clear legal foundation for each action taken is crucial, ensuring findings can be thoroughly explained and justified. Additionally, it is imperative to determine the type of evidence necessary to demonstrate non-compliance.

In Medicaid, relying solely on probabilistic models and risk scores was inadequate for an auditor's needs. While useful for initial assessments, these models did not provide the comprehensive and definitive information auditors need to conduct their work. For auditors to proceed with field audits, they require clear and complete findings. This means presenting claims and their context, accompanied by a narrative and policy rationale explicitly outlining why the transactions deviated from acceptable practices.

To address this need, we invested significant effort in documenting all analytic models, ensuring they were fully described in lay terms and could be referenced directly in the audit package used in fieldwork. This documentation served as a bridge between the probabilistic models and

the clear, definitive information required by auditors, ensuring that our findings were not only based on robust analytics but also presented in a manner that was accessible and understandable to the auditors.

While advanced analytic models are invaluable tools in identifying potential instances of non-compliance, the translation of these findings into a format that aligns with auditor expectations and requirements ultimately determines the success of the audit process. This translation requires careful documentation and presentation of findings, ensuring that every claim is backed by a clear rationale and supported by the necessary evidence.

In qualitative research evaluating the impacts of adding big data analysis to audit brainstorming sessions, Marei (2022) highlighted the positive effects of surfacing risk indicators to auditors. “Auditors… highlighted that the emerging Big Data is assessed in terms of its effect on the sufficiency, competence, and reliability of audit evidence. The evidence usually derived from the external context is more probabilistic and must be weighed in light of information’s characteristics.” It is essential to provide context and lineage to risk models to ensure auditors and downstream analysts can clearly understand them.

Over time, the partnership with audit firms and outside analysis further improved our library of analytic models and the breadth of improper activities detected. Kumaraswamy, Markey, and Ekin (2022) describe a functional anti-fraud team consisting of “trained and credentialed auditors, administrative/criminal investigators, statisticians/analysts/both, and investigative attorneys within any state or federal integrity programs” and suggest a “strong need for collaboration of the data team (statisticians/analysts/both) and the examiner’s (auditors, investigators, and attorneys) team to identify and convert fraud leads to recoupments.” We found this collaboration critical in Medicaid and worked to enable it through business processes that transparently communicated findings and case material to stakeholders.

Further, audits are typically an aggregated and prioritized list of findings. As S. Chen and Gangopadhyay (2013) state, “When setting the investigation targets after data analysis, we often take into consideration of the cost of

investigations and the potential ROI." This was top of mind for CMS in determining which providers to audit, prioritizing heavily on high potential recoupments.

Mehraby (2022) evaluates the claims analysis and target selection process for an Iranian health insurer using a dataset of 100k claims and evaluates the assessment process over the course of a year. It offers insight into approaches that could improve the targeting and assessment process, including the need for assessors to understand the methodology for the cases they are assigned clearly. It proposes clustering and rules association mining with visualization provided to assessors that can be clearly understood.

Rayan (2019) describes a hybrid framework for healthcare fraud detection, including a rules engine, supervised learning through decision trees and averaged perceptron, and unsupervised methods, such as clustering, outlier analysis, and k-means. The system provides auditors with a prioritized queue of claims with comments regarding why the claims are likely to be fraudulent. We took a similar approach with our Medicaid audits, arming auditors with claims data and model rationale they could test in the field.

7.3.6 Feedback

Feedback is the process of improving the overall system by integrating real-world testing of Findings (e.g., audit results), discovered data issues and opportunities (e.g., quality, veracity, new features/sources), new technologies, and evolving business context.

DP 6.1 Feedback and Improve

Design Principle	Feedback and Improve
Aim, implementer, and user	To enable an anti-fraud program (implementer) to improve program performance through operational and actor-domain learnings (aim) by data scientists, data engineers, subject matter experts, and auditors (enactors)
Context	In an operational fraud detection program
Mechanism	Incorporate learnings from model performance, technology innovations, new data collection approaches, and stakeholder partnerships through continuous improvement
Rationale	Because audited model results can help improve existing models and external opportunities can help shape future insights, improving program performance and impact.

The fields of technology, data collection, and analytical methods are in a state of constant evolution. This ongoing progress should influence not just the capabilities of fraud detection with existing data and processes but also warrant consideration for integration into operational systems.

In our Medicaid work, there was a continual effort to secure more accurate, timely, and reliable data. Our initial analyses relied on the MSIS dataset, a standardized, nationwide claims data collection. However, we quickly identified significant shortcomings in the dataset, particularly regarding feature definition. Medicaid is administered at the state level, with each state operating its own claims processing systems. These state systems are uniquely tailored to accommodate a state's specific policies and operational requirements. However, when the data from these diverse systems is consolidated into the national MSIS format, inconsistencies and disparities in data transformation and quality inevitably arise.

To address these issues, we proactively partnered with individual states to source authoritative claims and provider information directly from the state-based systems of record. This approach allowed us to bypass the data quality issues associated with the MSIS dataset. Additionally, it allowed us to manage and understand the complexities of mapping data across

different state systems on our terms. MSIS is one of many examples of iterative data-sourcing improvement undertaken with CMS. This proactive stance ensured that our work was grounded in the most accurate and reliable data available, enhancing our ability to detect and address fraud effectively.

Kumaraswamy, Markey, and Ekin (2022) state, “there is also a strong need for closing the feedback loop on what worked and what did not from an investigation and litigation standpoint.” Models need to be updated based on audit results to improve accuracy. Extensive work was done with the healthcare system's subject matter experts and stakeholders, including policy experts, prosecutors, providers, and auditors. With this feedback, we refined our models, improving our findings in subsequent analyses.

We worked to find ways to bridge principle-agent, information asymmetry, and incentive alignment challenges, seeking stakeholder cooperation wherever possible. This materialized in partnerships with states, with the federal government assisting in state interests, partnerships with other federal programs, such as Medicare, and collaboration with law enforcement and medical specialty associations, where appropriate. These partnerships led to better data, more informed guidance on approaches, and faster cycle times with analysis and audits.

Regarding technology evolutions, Nazir (2020) catalogs numerous research areas in healthcare big data management and analytics. Kumar and Singh (2019) and Pramanik (2022) highlight current big data technologies applicable to healthcare. Harerimana (2018) provides a survey of analytics technologies employed in healthcare. Bahri (2019) discusses current big data technologies and evaluates how they could impact various healthcare contexts, including “Healthcare monitoring, Healthcare Prediction, Recommendation systems, Healthcare Knowledge systems, and Healthcare Management Systems.” Significant innovation is at hand that can improve the quality of care, reduce costs, and improve outcomes. These technologies should be continuously evaluated for operational fraud detection system implementation.

Significant information asymmetry issues dominate the opportunities for fraudsters to commit fraud, and addressing these issues would make fraud

detection and prevention a much more straightforward problem. For example, can systemic structural changes in the claims process address data asymmetry and veracity issues? Saveetha and Maragatham (2022), W. Liu (2019), Gera (2020), Saldamli (2020), Ismail and Zeadally (2021), and Vyas (2022) discuss methods for incorporating blockchain-based distributed ledgers in the claims processing process to increase transparency and improve data veracity. This approach solves privacy concerns using currently available certificate and smart contract technologies and could be implemented in parallel or as the first step in claims processing operations.

Lakhan (2022) proposes using blockchain for healthcare Internet of Things (IoT) data storage and analysis for fraudulent data, exploring a layered approach to training and model application, beginning closer to the data source to reduce computational and energy costs. The computational performance characteristics of this approach were evaluated using healthcare provider claims to predict provider fraudulence based on training set data.

These and other technical innovations will no doubt shape the future of claims processing and enable new fraud detection approaches using better data. Practitioners should continuously review processes, actively seek feedback, identify relevant innovations, and consider their implementation in operational systems.

7.4 Conclusions

Fighting fraud, waste, and abuse in healthcare is a complex problem. The system is designed to deliver care and pay providers expediently. Detecting and preventing fraud was not a critical system design consideration, and, today, taxpayers suffer the consequence of this oversight in the form of billions of wasted government payments to fraudsters. This is, unfortunately, the case in many domains, and many changes are needed to improve the situation.

The design principles offered in this chapter propose guidance to fraud detection practitioners based on literature review and over a decade of field experience fighting fraud, developing partnerships, and learning what works (and does not) in the United States Medicaid healthcare system. The

principles are presented using Gregor's (Gregor et al., 2020) proposed design principle schema in relation to the steps of the KDD process. These principles distill key learnings into generalizable guidance applicable to healthcare fraud detection and other complex, multi-stakeholder domains.

8

Chapter 8: Conclusions and Future Research

Chapter 8: Conclusions and Future Research

8.1 Research Overview

1 in 6 dollars of GDP are spent on healthcare in the US. Annual spending continues to rise, averaging over a 9% increase each year since 2000, and this unsustainable spending growth has not brought better outcomes. The US spent 16% of GDP on healthcare in 2005, compared with an average of 9% across the remaining 30 OECD nations (WHO, 2008). The US ranked 29th in infant mortality, 25th in life expectancy, and 24th in maternal mortality, all out of these same 30 nations, in 2006 (Organization for Economic Cooperation and Development, 2006). This thesis offers approaches in fraud detection and employer plan management that can reduce costs and improve the value derived from spending in the US healthcare system.

Unsupervised data mining techniques such as outlier detection have been suggested as effective predictors for fraud. This thesis proposes and evaluates a model and techniques for healthcare fraud detection based on comparative research, fraud cases, and literature review. It also offers key design principles for fraud detection in complex systems distilled from learnings in Medicaid and literature. As presented in Chapter 1 and described in Figure 1, repeated below, the design science contribution is structured according to the Hevner et al. (Hevner et al., 2004) framework. It addresses a relevant and impactful problem in healthcare fraud detection and cost management.

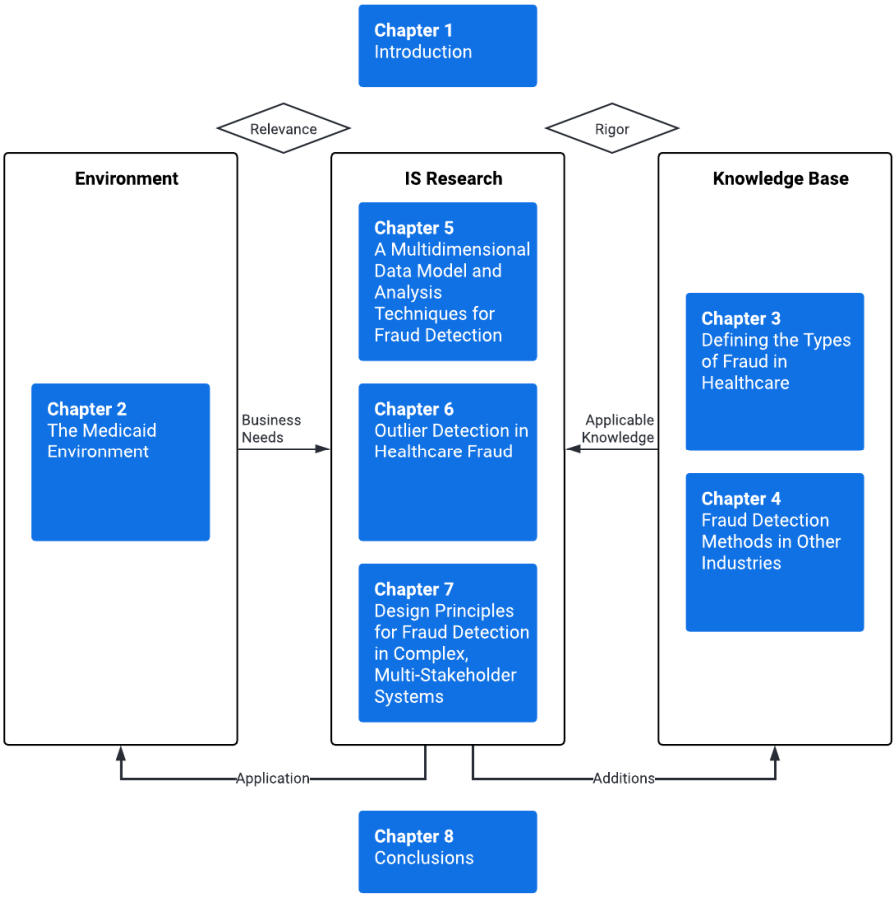


Figure 1 - Thesis Map

8.2 Results and Contributions

This thesis sought to develop models and methods to improve the state-of-the-art in healthcare fraud detection. Specifically, it offers the following contributions to the field:

1. A formal literature review of the field of fraud detection in Medicaid,
2. A multidimensional data model and analysis techniques for fraud detection in healthcare, including their applicability to the most prevalent known fraud types,
3. A framework for deploying outlier-based fraud detection methods in healthcare, and

4. Design principles for fraud detection in complex systems based on learnings in the Medicaid environment.

8.2.1 Literature Review

Chapters 3 and 4 offer formal reviews of the available literature on healthcare fraud. Chapter 3 focused on defining the types of fraud found in healthcare. Chapter 4 reviewed fraud detection techniques in literature across healthcare and other industries. Chapter 5 included a review of the literature covering fraud detection methodologies specifically utilized in healthcare.

8.2.2 Model and Techniques for Detecting Fraud in Healthcare

Chapter 5 developed a framework for fraud detection in Medicaid, providing specific data models and techniques to identify prevalent fraud schemes. Based on the analysis of the environment and knowledge base, a multidimensional schema based on Medicaid data was presented along with a set of multidimensional models and techniques to detect fraud in large sets of claim transactions. A typology of the applicability of these modes to the six most prevalent types of fraud was provided in Table 7. These artifacts were evaluated through functional testing against known fraud schemes. Chapter 5 contributed a set of multidimensional data models and analysis techniques that can be used to detect the most prevalent known fraud types.

8.2.3 A Framework for Outlier-Based Fraud Detection in Healthcare

Chapter 6 proposed and evaluated methods for applying outlier detection to healthcare fraud based on literature review, comparative research, direct application on healthcare claims data, and known fraudulent cases. Based on the multi-dimensional data model developed for Medicaid claim data (Thornton et al., 2013), a method for outlier-based fraud detection was presented and evaluated using Medicaid dental claims, providers, and patients in an actual US state Medicaid program.

Identifying 17 out of 360 (5%) primary dental providers statewide as warranting further investigation, of which 12 of 17 (71%) have been evaluated and deemed appropriate for formal investigation, is a level of success I would not have thought possible in the model's first revolution,

comparing with prior success rates in the field of roughly 10% (Major & Riedinger, 2002).

8.2.4 Design Principles for Fraud Detection in Complex, Multi-Stakeholder Systems

Chapter 7 offers key design principles to fraud detection practitioners in complex, multi-stakeholder systems, informed by literature and application in the US Medicaid healthcare system. These design principles are presented in reference to the KDD framework and distill key learnings from healthcare fraud detection to general principles applicable in other complex domains.

8.3 Research Limitations and Applicability

The characteristics of the US Medicaid system significantly shaped the progress and shape of my work and research contributions. Specifically, its multi-tier structure of state-run insurance systems primarily paid for by the federal government adds stakeholder misalignment, lack of architectural consistency, and policy differences that make fraud control extremely challenging at a federal level. These structural characteristics necessitated significant work from:

- state and federal fraud control organizations to prioritize targeting efforts,
- state Medicaid system subject matter experts to develop a shared understanding of critical data elements and policies,
- data engineers to map data from state formats to a more consistent view of this data nationally to enable cross-state analytics,
- healthcare subject matter experts to evaluate patterns of care, medical necessity, and appropriateness of care,
- data scientists to work with all of the above, applying data science techniques in concert with data and policy SMEs.

The research reflects our work to address unique systematic challenges in finding and fighting fraud, waste, and abuse. This work would be simplified in a less complex environment, such as a commercial insurer that controls its provider and patient populations, policies, and claims process, focusing more on SME-driven analytics and understanding a smaller population of

patients and providers. We demonstrated that a significant impact can be made, but working from a federal level to make inroads on Medicaid fraud is hard work spanning many disciplines.

Working in other industries across business functions since my efforts in Medicaid, I have seen the stakeholders change. However, the fundamental requirements for focusing on data veracity and building SME-driven data acquisition, engineering, and analytics capabilities have remained the same keys to sustainable success. These learnings were what I attempted to distill into a number of key design principles in Chapter 7.

My research was not focused on comparing the latest and greatest algorithms applied to healthcare fraud. I believe the status quo will continue to evolve on this front and that a future-proof approach must ensure that new approaches can be incorporated into past work. My focus was and is on how to build sustainable practices for applying data science and engineering to pressing business problems (in this case, healthcare fraud) to drive value.

One-off analytics projects can demonstrate a point and result in one-off returns. However, without focusing on operationalizing these efforts, they are merely shelfware, with little, if any, lasting impact. Model retraining, ensemble modeling, and ongoing ML Ops are essential to making incremental gains part of a long-term advance in the business practice.

Chapter 7 distills my research and learnings in Medicaid to more generalizable design principles I believe are applicable across industries. Figure 36 provides a consolidated visualization encapsulating key takeaways from years of work in this field.

8.4 Lessons Learned and Future Research

This research taught me much about antifraud efforts and the general applicability of research in other fields to Medicaid and healthcare. Significant healthcare subject matter expertise is required to design effective analysis techniques and interpret their results. The U.S. healthcare system is complicated. Better stakeholder incentive alignment, reduced information asymmetry, and improved communications and transparency are all needed to improve the healthcare system as a whole

and help transition it from an administrative, payment-centric model to a patient-centric one, mindful of fraud and waste prevention.

Applied research can improve this field and enhance fraud detection and prevention efforts, including evaluating graph and machine learning techniques relevant to healthcare fraud, data modeling, and people and process approaches to safeguarding trust in complex systems. This research hinges on data availability, which is problematic in an increasingly privacy-centric regulatory environment.

Despite the challenges, significant progress was achieved through this applied research in Medicaid, including material overpayments identified and recovered. The impacts of our efforts culminated in more significant investments in this space by CMS, unifying various Medicaid and Medicare anti-fraud activities to increase economies of scale and visibility across major parallel programs. In addition, I have found the generalized design principles discerned through working in Medicaid directly applicable in other multi-stakeholder domains, such as automotive warranty claims analysis.

With this research, I hope to have advanced the state of the art in healthcare fraud detection and prevention, materially assisted payers and law enforcement in confronting this significant societal challenge, and posited generalized design principles for fraud detection that span industries and can assist practitioners in other complex, multi-stakeholder domains.

R

References

Aggarwal, C. C. (2013). *Outlier analysis*. Springer.

Agrawal, S., Tarzy, B., Hunt, L., Taitsman, J., & Budetti, P. (2013). Expanding Physician Education in Health Care Fraud and Program Integrity: *Academic Medicine*, *88*(8), 1081–1087. https://doi.org/10.1097/ACM.0b013e318299f5cf

Ai, J., Russomanno, J., Guigou, S., & Allan, R. (2022). A Systematic Review and Qualitative Assessment of Fraud Detection Methodologies in Health Care. *North American Actuarial Journal*, *26*(1), 1–26. https://doi.org/10.1080/10920277.2021.1895843

Akbar, N. A., Sunyoto, A., Rudyanto Arief, M., & Caesarendra, W. (2020). Improvement of decision tree classifier accuracy for healthcare

insurance fraud prediction by using Extreme Gradient Boosting algorithm. *2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS)*, 110–114. https://doi.org/10.1109/ICIMCIS51567.2020.9354286

Alam, M. S., Tiwari, R. K., & Pandey, V. (2022). Healthcare Billing Fraud Detection Through Machine Learning And Using Homographic Encryption Technique For Prevention. *2021 4th International Conference on Recent Trends in Computer Science and Technology (ICRTCST)*, 181–186. https://doi.org/10.1109/ICRTCST54752.2022.9781896

Albrecht, W. S. (Ed.). (2012). *Fraud examination* (4th ed). South Western, Cengage Learning.

Alharbe, N., Rakrouki, M. A., & Aljohani, A. (2022). A Healthcare Quality Assessment Model Based on Outlier Detection Algorithm. *Processes*, *10*(6), Article 6. https://doi.org/10.3390/pr10061199

Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. *Applied Sciences*, *12*(19), Article 19. https://doi.org/10.3390/app12199637

Anbarasi, M. S., & Dhivya, S. (2017). Fraud detection using outlier predictor in health insurance data. *2017 International Conference on Information Communication and Embedded Systems (ICICES)*, 1–6. https://doi.org/10.1109/ICICES.2017.8070750

Aral, K. D., Güvenir, H. A., Sabuncuoğlu, İ., & Akar, A. R. (2012). A prescription fraud detection model. *Computer Methods and Programs in Biomedicine*, *106*(1), 37–46. https://doi.org/10.1016/j.cmpb.2011.09.003

Ashtiani, M. N., & Raahemi, B. (2022). Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review. *IEEE Access*, *10*, 72504–72525. https://doi.org/10.1109/ACCESS.2021.3096799

Bachhety, S., Singhal, R., & Jain, R. (2020). Intelligent Data Analysis with Data Mining. In *Intelligent Data Analysis* (pp. 63–83). John Wiley & Sons, Ltd. https://doi.org/10.1002/9781119544487.ch4

Baesens, B., Van Vlasselaer, V., & Verbeke, W. (2015). *An Economic Perspective on Fraud Analytics: Calculating ROI of Fraud Detection Systems*.

Bahri, S., Zoghlami, N., Abed, M., & Tavares, J. M. R. S. (2019). BIG DATA for Healthcare: A Survey. *IEEE Access*, *7*, 7397–7408. https://doi.org/10.1109/ACCESS.2018.2889180

Bauder, R. A., Herland, M., & Khoshgoftaar, T. M. (2019). Evaluating Model Predictive Performance: A Medicare Fraud Detection Case Study. *2019 IEEE 20th International Conference on Information Reuse and Integration for Data Science (IRI)*, 9–14. https://doi.org/10.1109/IRI.2019.00016

Bauder, R., Khoshgoftaar, T. M., & Seliya, N. (2017). A survey on the state of healthcare upcoding fraud analysis and detection. *Health Services and Outcomes Research Methodology*, *17*(1), 31–55. https://doi.org/10.1007/s10742-016-0154-8

Becker, R. A., Volinsky, C., & Wilks, A. R. (2010). Fraud Detection in Telecommunications: History and Lessons Learned. *Technometrics*, *52*(1), 20–33. https://doi.org/10.1198/TECH.2009.08136

Begoli, E., & Horey, J. (2012). Design Principles for Effective Knowledge Discovery from Big Data. *2012 Joint Working IEEE/IFIP Conference on Software Architecture and European Conference on Software Architecture*, pp. 215–218. https://doi.org/10.1109/WICSA-ECSA.212.32

Benbasat, I., Goldstein, D. K., & Mead, M. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, *11*(3), 369. https://doi.org/10.2307/248684

Bengio, Y., & Grandvalet, Y. (2003). No Unbiased Estimator of the Variance of K-Fold Cross-Validation. *Advances in Neural Information Processing Systems*, *16*. https://proceedings.neurips.cc/paper/2003/hash/e82c4b19b8151ddc25d4d93baf7b908f-Abstract.html

Bhattacharyya, S., Jha, S., Tharakunnel, K., & Westland, J. C. (2011). Data mining for credit card fraud: A comparative study. *Decision Support Systems*, *50*(3), 602–613. https://doi.org/10.1016/j.dss.2010.08.008

Boddy, A. J., Hurst, W., Mackay, M., & Rhalibi, A. el. (2019). Density-Based Outlier Detection for Safeguarding Electronic Patient Record Systems. *IEEE Access*, *7*, 40285–40294. https://doi.org/10.1109/ACCESS.2019.2906503

Bolton, R. J., & Hand, D. J. (2001). *Peer Group Analysis–Local Anomaly Detection in Longitudinal Data*. Citeseer. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.25.4115&rep=rep1&type=pdf

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, *17*(3), 235–255.

Bolton, R. J., Hand, D. J., & others. (1999). Unsupervised profiling methods for fraud detection. *Credit Scoring and Credit Control VII*.

Borca, G. (2001, April). Technology Curtails Health Care Fraud. *Managed Care*.

Cahill, M. H., Lambert, D., Pinheiro, J. C., & Sun, D. X. (2002). Detecting Fraud in the Real World. In J. Abello, P. M. Pardalos, & M. G. C. Resende (Eds.), *Handbook of Massive Data Sets* (Vol. 4, pp. 911–929). Springer US. http://link.springer.com/10.1007/978-1-4615-0005-6_26

Card, D., & Shore-Sheppard, L. D. (2004). Using Discontinuous Eligibility Rules to Identify the Effects of the Federal Medicaid Expansions on Low-Income Children. *Review of Economics and Statistics*, *86*(3), 752–766. https://doi.org/10.1162/0034653041811798

Carlson, J. (2013, April 12). Painful side effects. *Modern Healthcare*. http://www.modernhealthcare.com/article/20130412/MAGAZINE/304139973

Castaneda, G., Morris, P., & Khoshgoftaar, T. M. (2019). Maxout Neural Network for Big Data Medical Fraud Detection. *2019 IEEE Fifth*

International Conference on Big Data Computing Service and Applications (BigDataService), 357–362. https://doi.org/10.1109/BigDataService.2019.00064

Centers for Medicare and Medicaid Services. (2014). *Report to Congress: Fraud Prevention System Second Implementation Year*. https://www.stopmedicarefraud.gov/fraud-rtc06242014.pdf

Centers for Medicare and Medicaid Services. (2015). *Affordable Care Act*. Medicaid.Gov. http://medicaid.gov/affordablecareact/affordable-care-act.html

Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Comput. Surv.*, *41*(3), 15:1-15:58. https://doi.org/10.1145/1541880.1541882

Chen, M., Hao, Y., Hwang, K., Wang, L., & Wang, L. (2017). Disease Prediction by Machine Learning Over Big Data From Healthcare Communities. *IEEE Access*, *5*, 8869–8879. https://doi.org/10.1109/ACCESS.2017.2694446

Chen, S., & Gangopadhyay, A. (2013). A Novel Approach to Uncover Health Care Frauds through Spectral Analysis. *2013 IEEE International Conference on Healthcare Informatics*, 499–504. https://doi.org/10.1109/ICHI.2013.77

Churchill, W. (1939, October 1). *BBC Broadcast: The Russian Enigma*.

CMS. (n.d.). *National Health Expenditure Accounts*. https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsHistorical.html

CMS. (2020). *FY2020 Medicare and Medicaid PI Report to Congress (RTC)*.

Cohn, J. (2009, July 1). Your Health Care System: A Map. *The New Republic*. http://www.newrepublic.com/article/your-health-care-system-map

Colin, C., Ecochard, R., Delahaye, F., Landrivon, G., Messy, P., Morgon, E., & Matillon, Y. (1994). Data quality in a DRG-based information system. *International Journal for Quality in Health Care*, *6*(3), 275–280.

Copeland, L., Edberg, D., Panorska, A. K., & Wendel, J. (2012). Applying Business Intelligence Concepts to Medicaid Claim Fraud Detection. *Journal of Information Systems Applied Research*, *5*(1), 51.

Cunningham, P. J., & Hadley, J. (2008). Effects of Changes in Incomes and Practice Circumstances on Physicians' Decisions to Treat Charity

and Medicaid Patients. *The Milbank Quarterly*, *86*(1), 91–123. https://doi.org/10.1111/j.1468-0009.2007.00514.x

Cunningham, P. J., & May, J. H. (2006). *Medicaid Patients Increasingly Concentrated Among Physicians* (16).

Currie, J., & Gruber, J. (2001). Public health insurance and medical treatment: The equalizing impact of the Medicaid expansions. *Journal of Public Economics*, *82*(1), 63–89. https://doi.org/10.1016/S0047-2727(00)00140-7

Deeringer, P. A., Hellow, J. R., & Roth, R. L. (2012). *Tick, Tick, BOOM: CMS's Proposed 60-Day Rule Would Create Intense Time Pressure for Providers to Identify, Report, and Return Overpayments* (16 HFRA 167). Bloomberg BNA. http://www.bna.com/uploadedFiles/Content/Products/Books/HealthCareFraudReportArticle.pdf

Department of Health and Human Services. (2012). *Fiscal Year 2013 Budget in Brief*. https://wayback.archive-it.org/3920/20140403203145/http://www.hhs.gov/budget/fy2013/budget-brief-fy2013.pdf

Department of Health and Human Services. (1998). *Medicare A/B Reference Manual—Chapter 21—Benefit Integrity and Program*

Safeguard Contractors. https://http://www.novitas-solutions.com/refman/chapter-21.html

Department of Health and Human Services and Department of Justice. (2014). *The Department of Health and Human Services and The Department of Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2013*. http://oig.hhs.gov/publications/docs/hcfac/FY2013-hcfac.pdf

Department of Justice. (2011, April 14). *Miami Doctor Convicted in $23 Million Medicare Fraud Scheme*. Department of Justice - Justice News. http://www.justice.gov/opa/pr/miami-doctor-convicted-23-million-medicare-fraud-scheme

Department of Justice. (2012, February 27). *Los Angeles Church Pastor Sentenced to Serve 36 Months in Prison for $14.2 Million Medicare Fraud Scheme*. Department of Justice - Justice News. http://www.justice.gov/opa/pr/los-angeles-church-pastor-sentenced-serve-36-months-prison-142-million-medicare-fraud-scheme

Derrig, R. A. (2002). Insurance fraud. *Journal of Risk and Insurance*, *69*(3), 271–287.

Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020). A Secure AI-Driven Architecture for Automated Insurance Systems: Fraud Detection and Risk Measurement. *IEEE Access*, *8*, 58546–58558. https://doi.org/10.1109/ACCESS.2020.2983300

Dilla, W. N., & Raschke, R. L. (2015). Data visualization for fraud detection: Practice implications and a call for future research. *International Journal of Accounting Information Systems*, *16*, 1–22. https://doi.org/10.1016/j.accinf.2015.01.001

Dionne, G., Giuliano, F., & Picard, P. (2009). Optimal Auditing with Scoring: Theory and Application to Insurance Fraud. *Management Science*, *55*(1), 58–70. https://doi.org/10.1287/mnsc.1080.0905

District of New Jersey U.S. Attorneys Office. (2013, March 28). *South Jersey Doctor Admits Making Half-a-Million Dollars in Fraud Scheme Involving Home Health Care for Elderly Patients*. http://www.fbi.gov/newark/press-releases/2013/south-jersey-doctor-admits-making-half-a-million-dollars-in-fraud-scheme-involving-home-health-care-for-elderly-patients

District of Texas U.S. Attorneys Office. (2013). *Physician Pleads Guilty to Role in Health Care Fraud Conspiracy*.

http://www.fbi.gov/dallas/press-releases/2013/physician-pleads-guilty-to-role-in-health-care-fraud-conspiracy

DOJ. (2017). *Omnicare USDOJ Settlement*. https://www.justice.gov/usao-nj/press-release/file/966646/download

Dole, R. (Director). (1994, January 25). *State of the Union Response*. http://www.c-span.org/video/?54051-1/state-union-response

Dorn, S., Francis, N., Urban Institute, Snyder, L., & Rudowitz, R. (2015). *The Effects of the Medicaid Expansion on State Budgets: An Early Look in Select States*.

Dorronsoro, J. R., Ginel, F., Sgnchez, C., & Cruz, C. S. (1997). Neural fraud detection in credit card operations. *IEEE Transactions on Neural Networks*, *8*(4), 827–834. https://doi.org/10.1109/72.595879

Dube, J. F. (2011). Fraud in Health Care and Organized Crime. *Medicine & Health*, *94*(9), 268–269.

Duman, E. A., & Sağıroğlu, Ş. (2017). Health care fraud detection methods and new approaches. *2017 International Conference on Computer Science and Engineering (UBMK)*, 839–844. https://doi.org/10.1109/UBMK.2017.8093544

Ekin, T., Ieva, F., Ruggeri, F., & Soyer, R. (2018). Statistical Medical Fraud Assessment: Exposition to an Emerging Field: Statistical Methods

for Medical Fraud Assessment. *International Statistical Review*, *86*(3), 379–402. https://doi.org/10.1111/insr.12269

Fawcett, T., & Provost, F. (1997). Adaptive fraud detection. *Data Mining and Knowledge Discovery*, *1*(3), 291–316.

Fayyad, U., Piatetsky-Shapiro, G., & Smyth, P. (1996). The KDD process for extracting useful knowledge from volumes of data. *Communications of the ACM*, *39*(11), 27–34. https://doi.org/10.1145/240455.240464

Federal Bureau of Investigation. (2009). *Financial Crimes Report*. Federal Bureau of Investigation. http://www.fbi.gov/stats-services/publications/financial-crimes-report-2009

Ferreira, P., Alves, R., Belo, O., & Cortesão, L. (2006). Establishing Fraud Detection Patterns Based on Signatures. In P. Perner (Ed.), *Advances in Data Mining. Applications in Medicine, Web Mining, Marketing, Image and Signal Mining* (Vol. 4065, pp. 526–538). Springer Berlin Heidelberg. http://link.springer.com/10.1007/11790853_41

Forgionne, G. A., Gangopadhyay, A., & Adya, M. (2000). An intelligent data mining system to detect healthcare fraud. In A. Armoni, *Healthcare*

information systems: Challenges of the new millennium (pp. 148–169). IGI Global.

Freeman, B. A. & Loavenbruck, A. (2001). Complying with healthcare fraud laws: An overview for the hearing professional. *The Hearing Journal*, *54*(5).

Fu, K. K., Yang, M. C., & Wood, K. L. (2016). Design Principles: Literature Review, Analysis, and Future Directions. *Journal of Mechanical Design*, *138*(10). https://doi.org/10.1115/1.4034105

Fudenberg, D., & Maskin, E. (1986). The Folk Theorem in Repeated Games with Discounting or with Incomplete Information. *Econometrica*, *54*(3), 533–554. https://doi.org/10.2307/1911307

Furlan, Š., & Bajec, M. (2008). Holistic Approach to Fraud Management in Health Insurance. *Journal of Information and Organizational Sciences*, *32*(2), 99–114.

Fursov, I., Kovtun, E., Rivera-Castro, R., Zaytsev, A., Khasyanov, R., Spindler, M., & Burnaev, E. (2022). Sequence Embeddings Help Detect Insurance Fraud. *IEEE Access*, *10*, 32060–32074. https://doi.org/10.1109/ACCESS.2022.3149480

Gao, Y., Sun, C., Li, R., Li, Q., Cui, L., & Gong, B. (2018). An Efficient Fraud Identification Method Combining Manifold Learning and Outliers

Detection in Mobile Healthcare Services. *IEEE Access*, *6*, 60059–60068. https://doi.org/10.1109/ACCESS.2018.2875516

Garthwaite, C. L. (2012). The Doctor Might See You Now: The Supply Side Effects of Public Health Insurance Expansions. *American Economic Journal: Economic Policy*, *4*(3), 190–215. https://doi.org/10.1257/pol.4.3.190

Gera, J., Palakayala, A. R., Rejeti, V. K. K., & Anusha, T. (2020). Blockchain Technology for Fraudulent Practices in Insurance Claim Process. *2020 5th International Conference on Communication and Electronics Systems (ICCES)*, 1068–1075. https://doi.org/10.1109/ICCES48766.2020.9138012

Glied, S., & Ma, S. (2013). *How States Stand to Gain or Lose Federal Funds by Opting In or Out of the Medicaid Expansion*. The Commonwealth Fund.

Goldratt, E. M. (1990). *Haystack syndrome: Sifting information out of the data ocean.* North River Press.

Greer, J. L., Wood, J. J., Jensen, D. D., & Wood, K. L. (2008). *Guidelines for Product Evolution Using Effort Flow Analysis: Results of an Empirical Study*. 139–150. https://doi.org/10.1115/DETC2002/DTM-34013

Gregor, S., Kruse, L. C., & Seidel, S. (2020). Research Perspectives: The Anatomy of a Design Principle. *Journal of the Association for Information Systems*, *21*(6). https://doi.org/10.17705/1jais.00649

Grubbs, F. E. (1969). Procedures for detecting outlying observations in samples. *Technometrics*, *11*(1), 1–21.

Gruber, J., & Simon, K. (2008). Crowd-out 10 years later: Have recent public insurance expansions crowded out private health insurance? *Journal of Health Economics*, *27*(2), 201–217. https://doi.org/10.1016/j.jhealeco.2007.11.004

Gupta, P. (2017, June 5). *Cross-Validation in Machine Learning*. Medium. https://towardsdatascience.com/cross-validation-in-machine-learning-72924a69872f

Hampshire, K., Hamill, H., Mariwah, S., Mwanga, J., & Amoako-Sakyi, D. (2017). The application of Signalling Theory to health-related trust problems: The example of herbal clinics in Ghana and Tanzania. *Social Science & Medicine*, *188*, 109–118. https://doi.org/10.1016/j.socscimed.2017.07.009

Hancock, J., & Khoshgoftaar, T. M. (2020a). Medicare Fraud Detection using CatBoost. *2020 IEEE 21st International Conference on Information*

Reuse and Integration for Data Science (IRI), 97–103. https://doi.org/10.1109/IRI49571.2020.00022

Hancock, J., & Khoshgoftaar, T. M. (2020b). Performance of CatBoost and XGBoost in Medicare Fraud Detection. *2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA)*, 572–579. https://doi.org/10.1109/ICMLA51294.2020.00095

Hancock, J., & Khoshgoftaar, T. M. (2022). Optimizing Ensemble Trees for Big Data Healthcare Fraud Detection. *2022 IEEE 23rd International Conference on Information Reuse and Integration for Data Science (IRI)*, 243–249. https://doi.org/10.1109/IRI54793.2022.00061

Hand, D. J. (2010). Fraud Detection in Telecommunications and Banking: Discussion of Becker, Volinsky, and Wilks (2010) and Sudjianto et al. (2010). *Technometrics*, *52*(1), 34–38. https://doi.org/10.1198/TECH.2009.09115

Haque, M. E., & Tozal, M. E. (2022). Identifying Health Insurance Claim Frauds Using Mixture of Clinical Concepts. *IEEE Transactions on Services Computing*, *15*(4), 2356–2367. https://doi.org/10.1109/TSC.2021.3051165

Harerimana, G., Jang, B., Kim, J. W., & Park, H. K. (2018). Health Big Data Analytics: A Technology Survey. *IEEE Access*, *6*, 65661–65678. https://doi.org/10.1109/ACCESS.2018.2878254

Hast, R. H. (2000). *Health Care Fraud—Schemes to Defraud Medicare, Medicaid, and Private Health Care Insurers*. Subcommittee on Government Management, Information and Technology, Committee on Government Reform, House of Representatives.

Henderson, W. J. (2014). *Health economics and policy* (6th Ed). Cengage Learning.

Hernández, M. A., & Stolfo, S. J. (1998). Real-world Data is Dirty: Data Cleansing and The Merge/Purge Problem. *Data Mining and Knowledge Discovery*, *2*(1), 9–37. https://doi.org/10.1023/A:1009761603038

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75–105.

Hillerman, T. P., Carvalho, R. N., & Reis, A. C. B. (2015). Analyzing Suspicious Medical Visit Claims from Individual Healthcare Service Providers Using K-Means Clustering. In A. Kő & E. Francesconi (Eds.), *Electronic Government and the Information Systems Perspective*

(Vol. 9265, pp. 191–205). Springer International Publishing. http://link.springer.com/10.1007/978-3-319-22389-6_14

Holahan, J., Buettgens, M., Carroll, C., & Dorn, S. (2012). *The Cost and Coverage Implications of the ACA Medicaid Expansion: National and State-by-State Analysis*. Kaiser Commission on Medicaid and the Uninsured. http://kff.org/health-reform/report/the-cost-and-coverage-implications-of-the/

Holmström, B. (1979). Moral Hazard and Observability. *The Bell Journal of Economics*, *10*(1), 74–91. https://doi.org/10.2307/3003320

Hyman, D. A. (2001). Health Care Fraud and Abuse: Market Change, Social Norms, and the Trust" Reposed in the Workmen." *The Journal of Legal Studies*, *30*(2), 531–567.

Ismail, L., & Zeadally, S. (2021). Healthcare Insurance Frauds: Taxonomy and Blockchain-Based Detection Framework (Block-HI). *IT Professional*, *23*(4), 36–43. https://doi.org/10.1109/MITP.2021.3071534

Iyengar, V. S., Hermiz, K. B., & Natarajan, R. (2014). Computer-aided auditing of prescription drug claims. *Health Care Management Science*, *17*(3), 203–214. https://doi.org/10.1007/s10729-013-9247-x

Jain, R., & V, D. (2021). Data Mining Algorithms in Healthcare: An Extensive Review. *2021 Fifth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, 728–733. https://doi.org/10.1109/I-SMAC52330.2021.9640747

James D. Byrd Jr., Paige Powell, & Douglas L. Smith. (2013). Health Care Fraud: An Introduction to a Major Cost Issue. *Journal of Accounting, Ethics and Public Policy, 14*(3). http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2285860

Jing, R., Zheng, X., Tian, H., Zhang, X., Chen, W., Wu, D. D., & Zeng, D. D. (2019). A Graph-Based Semi-Supervised Fraud Detection Framework. *2019 4th IEEE International Conference on Cybernetics (Cybconf)*, 1–5. https://doi.org/10.1109/Cybconf47073.2019.9436573

Johnson, J. M., & Khoshgoftaar, T. M. (2020). Hcpcs2Vec: Healthcare Procedure Embeddings for Medicare Fraud Prediction. *2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, 145–152. https://doi.org/10.1109/CIC50333.2020.00026

Johnson, J. M., & Khoshgoftaar, T. M. (2022). Healthcare Provider Summary Data for Fraud Classification. *2022 IEEE 23rd International*

Conference on Information Reuse and Integration for Data Science (IRI), 236–242. https://doi.org/10.1109/IRI54793.2022.00060

Johnson, M. E., & Nagarur, N. (2016). Multi-stage methodology to detect health insurance claim fraud. *Health Care Management Science*, *19*(3), 249–260. https://doi.org/10.1007/s10729-015-9317-3

Joudaki, H., Rashidian, A., Minaei-Bidgoli, B., Mahmoodi, M., Geraili, B., Nasiri, M., & Arab, M. (2015). Using Data Mining to Detect Health Care Fraud and Abuse: A Review of Literature. *Global Journal of Health Science*, *7*(1), 194–202. https://doi.org/10.5539/gjhs.v7n1p194

Kaiser Commission on Medicaid and the Uninsured. (2012). *Health Insurance Coverage in America, 2011*. http://kff.org/slideshow/health-insurance-coverage-in-america-2011/

Kaiser Commission on Medicaid and the Uninsured. (2015a, April 20). *Current Status of Health Insurance Marketplace and Medicaid Expansion Decisions*. Kaiser Family Foundation. http://kff.org/health-reform/slide/current-status-of-health-insurance-marketplace-and-medicaid-expansion-decisions/

Kaiser Commission on Medicaid and the Uninsured. (2015b, April 29). *Current Status of State Medicaid Expansion Decisions*. Kaiser Family Foundation. http://kff.org/health-reform/slide/current-status-of-the-medicaid-expansion-decision/

Kaiser Family Foundation. (2015). *Recent Trends in Employer-Sponsored Insurance*. http://kff.org/slideshow/recent-trends-in-employer-sponsored-insurance/

Kapadiya, K., Patel, U., Gupta, R., Alshehri, M. D., Tanwar, S., Sharma, G., & Bokoro, P. N. (2022). Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects. *IEEE Access*, *10*, 79606–79627. https://doi.org/10.1109/ACCESS.2022.3194569

Kaplan, R. M., & Babad, Y. M. (2011). Balancing influence between actors in healthcare decision making. *BMC Health Services Research*, *11*(1), 85. https://doi.org/10.1186/1472-6963-11-85

Kareem, S., Binti Ahmad, R., & Sarlan, A. B. (2017). Framework for the identification of fraudulent health insurance claims using association rule mining. *2017 IEEE Conference on Big Data and Analytics (ICBDA)*, 99–104. https://doi.org/10.1109/ICBDAA.2017.8284114

Kelley, R. R. (2009). Where can $700 billion in waste be cut annually from the US healthcare system? *Ann Arbor, MI: Thomson Reuters*, *TR-7261 10/09 LW*.

Kou, Y., Lu, C. T., Sirwongwattana, S., & Huang, Y. P. (2005). Survey of fraud detection techniques. *Networking, Sensing and Control, 2004 IEEE International Conference On*, *2*, 749–754.

Krawczyk, M. (2009). The Role of Repetition and Observability in Deterring Insurance Fraud. *The Geneva Risk and Insurance Review*, *34*(1), 74–87. https://doi.org/10.1057/grir.2009.1

Kumar, S., & Singh, M. (2019). Big data analytics for healthcare industry: Impact, applications, and tools. *Big Data Mining and Analytics*, *2*(1), 48–57. https://doi.org/10.26599/BDMA.2018.9020031

Kumaraswamy, N., Markey, M. K., Barner, J. C., & Rascati, K. (2022). Feature engineering to detect fraud using healthcare claims data. *Expert Systems with Applications*, *210*, 118433. https://doi.org/10.1016/j.eswa.2022.118433

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), 1i.

Lakhan, A., Mohammed, M. A., Nedoma, J., Martinek, R., Tiwari, P., Vidyarthi, A., Alkhayyat, A., & Wang, W. (2022). Federated-Learning Based Privacy Preservation and Fraud-Enabled Blockchain IoMT System for Healthcare. *IEEE Journal of Biomedical and Health Informatics*, 1–1. https://doi.org/10.1109/JBHI.2022.3165945

Laleh, N., & Azgomi, M. A. (2009). A taxonomy of frauds and fraud detection techniques. In *Information Systems, Technology and Management* (pp. 256–267). Springer. http://link.springer.com/chapter/10.1007/978-3-642-00405-6_28

Li, J., Huang, K.-Y., Jin, J., & Shi, J. (2008). A survey on statistical methods for health care fraud detection. *Health Care Management Science*, *11*(3), 275–287. https://doi.org/10.1007/s10729-007-9045-4

Liang, C., Liu, Z., Liu, B., Zhou, J., Li, X., Yang, S., & Qi, Y. (2019). Uncovering Insurance Fraud Conspiracy with Network Learning. *Proceedings of the 42nd International ACM SIGIR Conference on Research and Development in Information Retrieval*, 1181–1184. https://doi.org/10.1145/3331184.3331372

Liu, W., Yu, Q., Li, Z., Li, Z., Su, Y., & Zhou, J. (2019). A Blockchain-Based System for Anti-Fraud of Healthcare Insurance. *2019 IEEE 5th*

International Conference on Computer and Communications (ICCC), 1264–1268. https://doi.org/10.1109/ICCC47050.2019.9064274

Liu, Y.-Y., Slotine, J.-J., & Barabási, A.-L. (2013). Observability of complex systems. *Proceedings of the National Academy of Sciences*, *110*(7), 2460–2465. https://doi.org/10.1073/pnas.1215508110

Lu, F., & Boritz, J. E. (2005). Detecting fraud in health insurance data: Learning to model incomplete Benford's law distributions. In *Machine Learning: ECML 2005* (pp. 633–640). Springer.

Luan, T., Yan, Z., & Zhang, S. (2019). Fraudster Detection Based on Modularity Optimization Algorithm. *2019 IEEE 23rd International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, 422–427. https://doi.org/10.1109/CSCWD.2019.8791908

Major, J. A., & Riedinger, D. R. (1992). EFD: A hybrid knowledge/statistical-based system for the detection of fraud. *International Journal of Intelligent Systems*, *7*(7), 687–703. https://doi.org/10.1002/int.4550070709

Major, J. A., & Riedinger, D. R. (2002). EFD: A Hybrid Knowledge/Statistical-Based System for the Detection of Fraud. *Journal of Risk and Insurance*, *69*(3), 309–324.

Marei, Y., Abu Afifa, M., Abdallah, A., Ayoush, M., & Amoush, A. (2022). Big Data and Big Data Analytics in Audit Brainstorming Sessions: A Canadian Qualitative Research. In S. G. Yaseen (Ed.), *Digital Economy, Business Analytics, and Big Data Analytics Applications* (pp. 657–671). Springer International Publishing. https://doi.org/10.1007/978-3-031-05258-3_51

Marijn G.A. Plomp & Jan H.A.M. Grijpink. (2011). Combating Identity Fraud in the Public Domain: Information Strategies for Healthcare and Criminal Justice. *Proceedings of the 11th European Conference on E-Government*, 451–458.

Matloob, I., & Khan, S. (2019). A Framework for Fraud Detection in Government Supported National Healthcare Programs. *2019 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, 1–7. https://doi.org/10.1109/ECAI46879.2019.9042126

Matloob, I., Khan, S. A., & Rahman, H. U. (2020). Sequence Mining and Prediction-Based Healthcare Fraud Detection Methodology. *IEEE Access*, *8*, 143256–143273. https://doi.org/10.1109/ACCESS.2020.3013962

Matloob, I., Khan, S. A., Rukaiya, R., Khattak, M. A. K., & Munir, A. (2022). A Sequence Mining-Based Novel Architecture for Detecting Fraudulent Transactions in Healthcare Systems. *IEEE Access*, *10*, 48447–48463. https://doi.org/10.1109/ACCESS.2022.3170888

Mavlanova, T., Benbunan-Fich, R., & Koufaris, M. (2012). Signaling theory and information asymmetry in online commerce. *Information & Management*, *49*(5), 240–247. https://doi.org/10.1016/j.im.2012.05.004

Mehraby, N., Neysiani, B. S., Nogorani, M. Z., & Ataabadi, P. E. (2022). Abnormal Behavior Detection in Health Insurance Assessment Process. *2022 8th International Conference on Web Research (ICWR)*, 76–81. https://doi.org/10.1109/ICWR54782.2022.9786232

Meng, Y., Qin, T., Li, S., & Wang, P. (2022). Behavior Pattern Mining from Traffic and Its Application to Network Anomaly Detection. *Security and Communication Networks*, *2022*, e9139321. https://doi.org/10.1155/2022/9139321

Moreau, Y., Shawe-taylor, P. B. J., & Stoermann, C. (1996). *Novel Techniques for Fraud Detection in Mobile Telecommunication Networks*. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.48.1207

Morris, L. (2009). Combating Fraud In Health Care: An Essential Component Of Any Cost Containment Strategy. *Health Affairs*, *28*(5), 1351–1356. https://doi.org/10.1377/hlthaff.28.5.1351

Musal, R. M. (2010). Two models to investigate Medicare fraud within unsupervised databases. *Expert Systems With Applications*, *37*(12), 8628–8633. https://doi.org/10.1016/j.eswa.2010.06.095

National Association of Medical Fraud Control Units. (2013). *NAMFCU Medicaid Fraud Reports*. http://www.namfcu.net/resources/medicaid-fraud-reports-newsletters/

Nazir, S., Khan, S., Khan, H. U., Ali, S., García-Magariño, I., Atan, R. B., & Nawaz, M. (2020). A Comprehensive Analysis of Healthcare Big Data Management, Analytics and Scientific Programming. *IEEE Access*, *8*, 95714–95733. https://doi.org/10.1109/ACCESS.2020.2995572

Nazir, S., Nawaz, M., Adnan, A., Shahzad, S., & Asadi, S. (2019). Big Data Features, Applications, and Analytics in Cardiology—A Systematic Literature Review. *IEEE Access*, *7*, 143742–143771. https://doi.org/10.1109/ACCESS.2019.2941898

Ng, K. S., Shan, Y., Murray, D. W., Sutinen, A., Schwarz, B., Jeacocke, D., & Farrugia, J. (2010). Detecting Non-compliant Consumers in Spatio-Temporal Health Data: A Case Study from Medicare Australia. *Data Mining Workshops (ICDMW), 2010 IEEE International Conference On*, 613–622.

Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, *50*(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006

Nowack, M. L. (1997). *Design guidelines for manufacturability* [Thesis, University of Cambridge]. https://doi.org/10.17863/CAM.14133

ObamacareFacts.com. (2015, May 1). *ObamaCare Essential Health Benefits*. ObamacareFacts.Com. http://obamacarefacts.com/essential-health-benefits/

Ogunbanjo, G. A. & Knapp van Bogaert, D. (2014). Ethics in health care: Healthcare fraud: Ethics CPD supplement. *South African Family Practice*, *56*(1), S10–S13.

Omair, B., & Alturki, A. (2020). A Systematic Literature Review of Fraud Detection Metrics in Business Processes. *IEEE Access*, *8*, 26893–26903. https://doi.org/10.1109/ACCESS.2020.2971604

Organisation for Economic Co-operation and Development. (2012). *OECD health data October 2012*. http://www.oecd.org/els/health-systems/OECDHealthData2012FrequentlyRequestedData_Updated_October.xls

Organization for Economic Cooperation and Development. (2006). *OECD Health Data 2009: Statistics and Indicators for 30 Countries*.

Ortega, P. A., Figueroa, C. J., & Ruz, G. A. (2006). A Medical Claim Fraud/Abuse Detection System based on Data Mining: A Case Study in Chile. *Proceedings of the 2006 International Conference on Data Mining*, 224–231.

Panigrahi, P. K. (2011). A Framework for Discovering Internal Financial Fraud Using Analytics. *2011 International Conference on Communication Systems and Network Technologies*, 323–327. https://doi.org/10.1109/CSNT.2011.74

Patient Protection and Affordable Care Act, Pub. L. No. 111–148, 42 U.S.C. (2010). http://www.gpo.gov/fdsys/pkg/PLAW-111publ148/content-detail.html

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *arXiv Preprint arXiv:1009.6119*.

Pincus, R. (1995). Barnett, V., and Lewis T.: Outliers in Statistical Data. 3rd edition. J. Wiley & Sons 1994, XVII. 582 pp., £49.95. *Biometrical Journal*, *37*(2), 256–256. https://doi.org/10.1002/bimj.4710370219

Pramanik, P. K. D., Pal, S., & Mukhopadhyay, M. (2022). *Healthcare Big Data: A Comprehensive Overview* [Chapter]. Research Anthology on Big Data Analytics, Architectures, and Applications; IGI Global. https://doi.org/10.4018/978-1-6684-3662-2.ch006

Provost, F., & Fawcett, T. (2013). Data Science and its Relationship to Big Data and Data-Driven Decision Making. *Big Data*, *1*(1), 51–59. https://doi.org/10.1089/big.2013.1508

Purandhar, N., Ayyasamy, S., & Siva Kumar, P. (2022). Classification of clustered health care data analysis using generative adversarial

networks (GAN). *Soft Computing*, *26*(12), 5511–5521. https://doi.org/10.1007/s00500-022-07026-7

Rabecs, R. (2006). Health care fraud under the new Medicare Part D prescription drug program. *The Journal of Criminal Law and Criminology*, *96*(2), 727–756.

Rashidian, A., Joudaki, H., & Vian, T. (2012). No Evidence of the Effect of the Interventions to Combat Health Care Fraud and Abuse: A Systematic Review of Literature. *PLoS ONE*, *7*(8), e41988. https://doi.org/10.1371/journal.pone.0041988

Rawte, V., & Anuradha, G. (2015). Fraud detection in health insurance using data mining techniques. *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*, 1–5. https://doi.org/10.1109/ICCICT.2015.7045689

Rayan, N. (2019). Framework for Analysis and Detection of Fraud in Health Insurance. *2019 IEEE 6th International Conference on Cloud Computing and Intelligence Systems (CCIS)*, 47–56. https://doi.org/10.1109/CCIS48116.2019.9073700

Rose, S. (2015). Opting In, Opting Out: The Politics of State Medicaid Expansion. *The Forum*, *13*(1). https://doi.org/10.1515/for-2015-0011

Rousseeuw, P. J., & van Zomeren, B. C. (1990). Unmasking Multivariate Outliers and Leverage Points. *Journal of the American Statistical Association*, *85*(411), 633–639.

Rumsfeld, D. (2002). *Secretary Rumsfeld Press Conference at NATO Headquarters* [Interview]. http://www.defense.gov/transcripts/transcript.aspx?transcriptid=3490

National Federation of Independent Business v. Sebelius, 132 S. Ct. 2566 (Supreme Court 2012).

Sadiq, S., Tao, Y., Yan, Y., & Shyu, M.-L. (2017). Mining Anomalies in Medicare Big Data Using Patient Rule Induction Method. *2017 IEEE Third International Conference on Multimedia Big Data (BigMM)*, 185–192. https://doi.org/10.1109/BigMM.2017.56

Saldamli, G., Reddy, V., Bojja, K. S., Gururaja, M. K., Doddaveerappa, Y., & Tawalbeh, L. (2020). Health Care Insurance Fraud Detection Using Blockchain. *2020 Seventh International Conference on Software Defined Systems (SDS)*, 145–152. https://doi.org/10.1109/SDS49854.2020.9143900

Saveetha, D., & Maragatham, G. (2022). A Decentralized Blockchain based system for Secure Health Record and Claims processing. *2022*

International Conference on Computer Communication and Informatics (ICCCI), 1–8. https://doi.org/10.1109/ICCCI54379.2022.9740838

Schwartz, R. B., & Russo, M. C. (2004). How to quickly find articles in the top IS journals. *Communications of the ACM*, *47*(2), 98. https://doi.org/10.1145/966389.966417

Settipalli, L., & Gangadharan, G. R. (2023). WMTDBC: An unsupervised multivariate analysis model for fraud detection in health insurance claims. *Expert Systems with Applications*, *215*, 119259. https://doi.org/10.1016/j.eswa.2022.119259

Settipalli, L., Gangadharan, G. R., & Fiore, U. (2022). Predictive and adaptive Drift Analysis on Decomposed Healthcare Claims using ART based Topological Clustering. *Information Processing & Management*, *59*(3), 102887. https://doi.org/10.1016/j.ipm.2022.102887

Shan, Y., Jeacocke, D., Murray, D. W., & Sutinen, A. (2008). Mining Medical Specialist Billing Patterns for Health Service Management. *Proceedings of the 7th Australasian Data Mining Conference - Volume 87*, 105–110.

Shin, H., Park, H., Lee, J., & Jhee, W. C. (2012). A scoring model to detect abusive billing patterns in health insurance claims. *Expert Systems with Applications*, *39*(8), 7441–7450.

S.K., S., & Ilango, V. (2020). A time-efficient model for detecting fraudulent health insurance claims using Artificial neural networks. *2020 International Conference on System, Computation, Automation and Networking (ICSCAN)*, 1–6. https://doi.org/10.1109/ICSCAN49426.2020.9262298

Skillicorn, D. B. (2009). Adversarial Knowledge Discovery. *IEEE Intelligent Systems*, *24*(6), 54–61. https://doi.org/10.1109/MIS.2009.108

Sommers, B. D., Baicker, K., & Epstein, A. M. (2012). Mortality and Access to Care among Adults after State Medicaid Expansions. *New England Journal of Medicine*, *367*(11), 1025–1034. https://doi.org/10.1056/NEJMsa1202099

Sparer, M. (2012). Medicaid managed care: Costs, access, and quality of care. *POLICY*, *1*, 6.

Sparrow, M. K. (2000). *License to steal: How fraud bleeds America's health care system* (Updated ed). Westview Press.

Sparrow, M. K. (2008). Fraud in the US Health-Care System: Exposing the Vulnerabilities of Automated Payments Systems. *Social Research: An International Quarterly*, *75*(4), 1151–1180.

Stanton, T. H. (2001). Fraud-And-Abuse Enforcement In Medicare: Finding Middle Ground. *Health Affairs*, *20*(4), 28–42. https://doi.org/10.1377/hlthaff.20.4.28

Sudjianto, A., Nair, S., Yuan, M., Zhang, A., Kern, D., & Cela-Díaz, F. (2010). Statistical Methods for Fighting Financial Crimes. *Technometrics*, *52*(1), 5–19.

Sun, C., Li, Q., Li, H., Shi, Y., Zhang, S., & Guo, W. (2019). Patient Cluster Divergence Based Healthcare Insurance Fraudster Detection. *IEEE Access*, *7*, 14162–14170. https://doi.org/10.1109/ACCESS.2018.2886680

Sun, C., Yan, Z., Li, Q., Zheng, Y., Lu, X., & Cui, L. (2019). Abnormal Group-Based Joint Medical Fraud Detection. *IEEE Access*, *7*, 13589–13596. https://doi.org/10.1109/ACCESS.2018.2887119

Sunzi, & Giles, L. (2005). *The art of war*. El Paso Norte Press.

Tang, M., Mendis, B. S. U., Murray, D. W., Hu, Y., & Sutinen, A. (2011). Unsupervised fraud detection in Medicare Australia. *Proceedings of*

the Ninth Australasian Data Mining Conference-Volume 121, 103–110.

The R Foundation. (2015). *The R project for statistical computing*. http://www.r-project.org/

Thomas, R., & Judith, J. E. (2020). Hybrid Outlier Detection in Healthcare Datasets using DNN and One Class-SVM. *2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA)*, 1293–1298. https://doi.org/10.1109/ICECA49313.2020.9297401

Thompson/MEDSTAT. (2005, April). *Medicaid Estate Recovery*. U.S. Department of Health and Human Services.

Thornton, D., Brinkhuis, M., Amrit, C., & Aly, R. (2015, May). *Categorizing and Describing the Types of Fraud in Healthcare*. submitted to Conference on Health and Social Care Information Systems and Technologies.

Thornton, D., Mueller, R. M., Schoutsen, P., & van Hillegersberg, J. (2013). Predicting Healthcare Fraud in Medicaid: A Multidimensional Data Model and Analysis Techniques for Fraud Detection. *Procedia Technology*, *9*, 1252–1264.

Thornton, D., van Capelleveen, G. C., van Hillegersberg, J., & Mueller, R. M. (2014). Outlier-based Health Insurance Fraud Detection for U.S. Medicaid Data. *Proceedings of the 16th International Conference on Enterprise Information Systems (ICEIS 2014)*, 684–694.

Tow, T. H. (2011). *Squeezing through Obamacare: The battle of carrots, sticks, and sermons* [University of Hong Kong]. http://dx.doi.org/10.5353/th_b4694230

Travaille, P., Müller, R. M., Thornton, D., & Hillegersberg, J. (2011). *Electronic Fraud Detection in the US Medicaid Healthcare Program: Lessons Learned from other Industries*.

Truffer, C. J., Klemm, J. D., Wolfe, C. J., Rennie, K. E., & Shuff, J. F. (2013). *2013 Actuarial Report on the Financial Outlook for Medicaid*. Department of Health & Human Services. http://medicaid.gov/medicaid-chip-program-information/ by-topics/financing-and-reimbursement/downloads /medicaid-actuarial-report-2013.pdf

Turban, E., Sharda, R., & Delen, D. (2011). *Decision support and business intelligence systems* (9th ed). Prentice Hall.

United States Attorney's Office for the Central District of California. (2012, May 2). *8 Los Angeles-Area Residents Charged In Nationwide*

Medicare Fraud Strike Force Takedown [Government]. United States Attorney's Office for the Central District of California. http://www.justice.gov/usao/cac/Pressroom/2012/055.html

U.S. Federal Bureau of Investigation. (2013). *FBI news blog*. http://www.fbi.gov/news/news_blog

U.S. Government Accountability Office. (2012). *Medicare Fraud Prevention: CMS has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine its Effectiveness*. http://www.gao.gov/products/GAO-13-104

U.S. Office Inspector General, & Murrin, S. (2015). *Questionable billing for Medicaid pediatric dental services in California*. http://oig.hhs.gov/oei/reports/oei-02-14-00480.pdf

Verma, A., Taneja, A., & Arora, A. (2017). Fraud detection and frequent pattern matching in insurance claims using data mining techniques. *2017 Tenth International Conference on Contemporary Computing (IC3)*, 1–7. https://doi.org/10.1109/IC3.2017.8284299

Vyas, S., & Serasiya, S. (2022). Fraud Detection in Insurance Claim System: A Review. *2022 Second International Conference on Artificial Intelligence and Smart Energy (ICAIS)*, 922–927. https://doi.org/10.1109/ICAIS53314.2022.9742984

Vyas, S., Serasiya, S., & Vyas, A. (2022). Combined Approach of ML and Blockchain for Fraudulent Detection in Insurance Claim. *2022 International Conference on Edge Computing and Applications (ICECAA)*, 544–550. https://doi.org/10.1109/ICECAA55415.2022.9936353

Wang, L., Hu, W., Zheng, T., Yin, S., Zhang, X., & Liu, X. (2022). Node Similarity-based Search Method for Medical Insurance Heterogeneous Information Network. *2022 IEEE 8th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 174–179. https://doi.org/10.1109/BigDataSecurityHPSCIDS54978.2022.00041

Who. (2008). *World health statistics 2008*. World Health Organization.

Yamanishi, K., Takeuchi, J.-I., Williams, G., & Milne, P. (2004). On-line unsupervised outlier detection using finite mixtures with discounting learning algorithms. *Data Mining and Knowledge Discovery*, *8*(3), 275–300.

Yang, W.-S., & Hwang, S.-Y. (2006). A process-mining framework for the detection of healthcare fraud and abuse. *Expert Systems with Applications*, *31*(1), 56–68.

Yao, J., Yu, S., Wang, C., Ke, T., & Zheng, H. (2021). Medicare Fraud Detection Using WTBagging Algorithm. *2021 7th International Conference on Computer and Communications (ICCC)*, 1515–1519. https://doi.org/10.1109/ICCC54389.2021.9674545

Yin, R. K. (2011). Case Study Research: Design and Methods by YIN, ROBERT K. *The Modern Language Journal*, *95*(3), 474–475. https://doi.org/10.1111/j.1540-4781.2011.01212_17.x

Yoo, Y., Shin, D., Han, D., Kyeong, S., & Shin, J. (2022). Medicare fraud detection using graph neural networks. *2022 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, 1–5. https://doi.org/10.1109/ICECET55527.2022.9872963

Zhang, J., Yang, F., Lin, K., & Lai, Y. (2022). Hierarchical Multi-Modal Fusion on Dynamic Heterogeneous Graph for Health Insurance Fraud Detection. *2022 IEEE International Conference on Multimedia and Expo (ICME)*, 1–6. https://doi.org/10.1109/ICME52920.2022.9859871

Zhang, W., Liu, X., Zhang, X., Hu, W., Zhang, J., & Shao, W. (2022). Medicare Fraud Gang Discovery Based on Community Discovery Algorithms. *2022 IEEE 8th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, 206–211. https://doi.org/10.1109/BigDataSecurityHPSCIDS54978.2022.00047

Zhao, B., Shi, Y., Zhang, K., & Yan, Z. (2019). Health Insurance Anomaly Detection Based on Dynamic Heterogeneous Information Network. *2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM)*, 1118–1122. https://doi.org/10.1109/BIBM47256.2019.8983130

Zhou, S., & Zhang, R. (2020). A Novel Method for Mining Abnormal Expenses in Social Medical Insurance. *2020 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*, 1–5. https://doi.org/10.1109/IEMTRONICS51293.2020.9216354

Zhu, S., Wang, Y., & Wu, Y. (2011). Health care fraud detection using nonnegative matrix factorization. *2011 6th International*

Conference on Computer Science & Education (ICCSE), 499–503.

https://doi.org/10.1109/ICCSE.2011.6028688