IMPROVING THE PROCESSES AND SAFEGUARDS FOR FRAUD DETECTION AND PREVENTION IN US MEDICAID

MASTER THESIS

Combating white-collar crime in US healthcare programs

Patrick M. Höner
Business Information Technology
Faculty of Electrical Engineering,
Mathematics and Computer Science

December 20, 2015
Enschede

UNIVERSITY OF TWENTE.

UC San Diego

Improving the Processes and Safeguards for Fraud Detection and Prevention in US Medicaid

Combating white-collar crime in US healthcare programs

Enschede, December 20, 2015

Author

Patrick M. Höner
Study Program *Business Information Technology*
Faculty of Electrical Engineering,
Mathematics and Computer Science

Student No. 1013173
E-mail p.m.hoener@alumnus.utwente.nl

Graduation Committee

Jos van Hillegersberg, Prof. Dr.
Department Industrial Engineering and Business Information Systems
E-mail j.vanhillegersberg@utwente.nl

Marten van Sinderen, Dr. ir.
Department Electrical Engineering, Mathematics and Computer Science
E-mail m.j.vansinderen@utwente.nl

Dallas Thornton, PhD
Clemson University
E-mail dallas@clemson.edu

Preface

This thesis concludes my life as a student at the University of Twente and as intern at the San Diego Supercomputer Center, UC San Diego. The past few months have been devoted to reading, researching, talking, hearing and writing about fraud in US Medicaid. In this journey, I have learned a lot about what Medicaid fraud is, what constitutes to its occurrence, and why combating fraud in healthcare remains a challenge. The last year has also been about balancing academic precision with working life. I received help from many people with various topics and I would like to thank a few of them explicitly.

Completion of this study would not have been possible without the generous and unwavering support of my graduation committee. I wish to express my deepest gratitude to my supervisors, Jos van Hillegersberg and Maarten van Sinderen, for their guidance, encouragement, wisdom, and valuable insights throughout this research project. Their critical review helped me to improve the clarity and presentation of my work.

I also want to thank the people who helped me to validate and complete the findings of this research. I thank the participants in my study for their contributions and their candor.

A special thanks goes to the SDSC and the people that I had the pleasure of working with this past year, and who helped me to explore the subject domain and find my way through the misty start of this graduation project.
I hereby like to thank Peter and Danielle for their guidance and integration into the project. I would also like to thank Dallas Thornton and Sandeep Chandra for granting me the possibility of working in the US. Further I would like to thank Christopher Battistuz for his effort and unlimited support.

Finally, I would like to thank my friends and family for their feedback and support throughout the past months and for all the years before.

For now, I hope you enjoy reading through my thesis as much as I enjoyed writing it.

Patrick Hoener,

Münster, December 7, 2015

Abstract

Healthcare costs in the United States are higher than anywhere else in the world. One of the reasons that constitutes to such high costs that account for almost 20% of the country's GDP is healthcare fraud. Medicaid is a jointly funded, state administered healthcare program for low-income adults, children, pregnant women, elderly adults and people with disabilities. Because of its structural features and distributed control, the Medicaid program is extremely susceptible to fraud.

This paper describes the organizational context of the fraud control setting in Medicaid, and process and technological aspects that define current state and its effectiveness. Literature and document review utilizing open coding, and process mining applied on a work system in use allow for a comprehensive holistic overview on Medicaid fraud control.

Four major control systems were identified, while the fraud control process defines the control span between initial claim inception at State Medicaid Agencies, federal postpayment review and potential fraud referral.
Investigating the processes and safeguards in detail along with roles and responsibilities of the parties involved, a number of limitations were identified that severely mitigate current efforts to protect the Medicaid fund from improper payments and, most significantly, fraud.

A set of actions was defined to improve the processes and safeguards targeting the process, technological and organizational setting.
In two interviews with experts these limitations were validated, and requirements for change and actions for de-limitations discussed.

Recommendations include requiring state agencies to implement predictive analytics systems, modernize state IT architecture, and increase Manual Review during prepayment processing.

More research is needed to assess the perception of fraud control at state level, and to identify policy implications for change. As for practice, political actions are needed to enforce a set of actions to be taken, not to keep relying on the distributed and passive control, without clear incentives of finding fraud.

In the future, without a fundamental coordinated control strategy, the Medicaid fund will remain susceptible to fraudsters.

keywords: Medicaid fraud control, processes, safeguards, healthcare, fraud, prevention, fraud prediction

Table of Contents

Preface 5
Abstract 6
Table of Contents 7
List of Figures 8
List of Tables 8
Glossary 9
1 Introduction 11
1.1 Background of the problem 14
1.1.1 Medicare, Medicaid and fraud 14
1.1.2 Technology perspective 14
1.1.3 A natural target 15
1.1.4 Fraud perpetrators and schemes in healthcare 15
1.1.5 Severity and consequences of fraud in healthcare 16
1.1.6 Medicare and Medicaid fraud and abuse laws 17
1.1.7 HIPAA 18
1.1.8 Fraud control in a hostile environment 18
1.1.9 Fraud detection versus fraud prevention 19
1.2 Research Design 20
1.2.1 Problem Statement 20
1.2.2 Research Objective 20
1.2.3 Research Scope and Subject Domain 21
1.2.4 Research Questions 21
1.3 Document Structure 23
2 Conceptual framework 25
3 Literature Review 28
4 Safeguards and Processes in Medicaid // AS IS 33
4.1 Control systems 33
4.1.1 Prepayment Review vs. Postpayment Review 34
4.1.2 Claim Processing / Edits and Audits 35
4.1.3 Prepayment Medical Review / Manual Claim Review 38
4.1.4 Postpayment Utilization Review / Cost Control Audits 39
4.1.5 Special Investigative Units / Audits 40
4.1.6 Review 40
4.2 Program Oversight at State and Federal level 41
4.2.1 State Medicaid Agency, CMS, OIG and MFCU 41
4.2.2 Contractors 44
4.2.3 Review 46
4.3 Horizontal process view – Holistic perspective 47
4.4 Intra and Inter-Organizational Processes Refined 49
4.4.1 Prepayment processes 49
4.4.2 Postpayment processes 52
4.5 Timeline perspective 57
4.6 Medicaid state data and CMS data sources 58
4.7 Review and Discussion - Bringing the pieces together 59
5 Gaps in current Medicaid Safeguards 61

5.1 Prepayment gaps 62
5.3 Post-payment gaps 66
5.4 Discussion & Review 69
6 Improving Processes and Safeguards // TO BE 71
6.1 Prepayment safeguards 71
6.2 Postpayment safeguards 77
6.3 Review 81
7 Validation 83
7.1 Validation grounds 83
7.2 Interview questions 83
7.3 Validation results 85
7.3.1 Interview #1 85
7.3.2 Interview #2 88
8 Discussion 90
9 Conclusion 92
9.1 Conclusions 92
9.2 Contribution 95
9.3 Limitations 96
9.4 Future Work 96
References 98

List of Figures

Figure 1 - Spectrum of Fraud (Agrawal et al., 2013) 12
Figure 2 - Research methodology 22
Figure 3 - Conceptual framework 27
Figure 4 - Themes in literature 30
Figure 5 - Control systems in Medicaid 34
Figure 6 - Control system in organizational context 46
Figure 7 - Process View Prepayment (Control systems 1 and 2) 47
Figure 8 - Process View Postpayment (Control systems 3 and 4) 48
Figure 9 - Claims processing process 50
Figure 10 - Automated Review Edits & Audits 51
Figure 11 - Data transfer from State to Federal level 52
Figure 12 - CMS postpayment review process 54
Figure 13 - The timeline of the fraud control process 58
Figure 14 - Federal initiative for national Medicaid data sharing 74
Figure 15 - Proposed fraud control process at prepayment level 77
Figure 16 - Iterative in-house auditing 79

List of Tables

Table 1 - Types of Fraud 16
Table 2 - Document and research overview 24
Table 3 - Themed limitations 93

Glossary

ACA	Affordable Care Act
Beneficiary	An individual entitles to receive medical care under a certain program
BPMN	Business Process Modeling Notation
CMS	Centers for Medicaid and Medicare Services, federal agency under HHS administering the Medicare and Medicaid (together with states) programs.
CPI	Center for Program Integrity, division of CMS, focal point for Medicare and Medicaid integrity anti fraud and abuse efforts
CFR	Code of Federal Regulations
Fiscal agent	Private contractor to the state - normally selected through a call for bids for a defined duration - operating the state's MMIS
FPS	Fraud Prevention System, predictive analytics system for Medicare program, implementation started 2011
GAO	Government Accountability Office
HHS	US Department of Health & Human Services
Insurer	Any health program that helps pay for medical expenses, to provide protection against the costs of medical services needed.
Medicaid	A jointly funded, state administered healthcare program for low-income adults, children, pregnant women, elderly adults and people with disabilities.
Medicare	A federally funded and administered healthcare program for Americans 65 years of age or older.
MFCU	Medicaid Fraud Control Unit, agency for statewide provider fraud investigations
MIC	Medicaid Integrity Contractor (Review MIC, Audit MIC, Education MIC)
MIG	Medicaid Integrity Group, responsible for implementing the MIP, operating within CPI, until 2014
MIP	Medicaid Integrity Program; Deficit Reduction Act of 2005 established the MIP as a first comprehensive Federal strategy to prevent and reduce provider fraud, waste, and abuse
MMIS	Medicaid Management Information System, central Information System and focal point used by State Agency for beneficiary services, providers and inquired, claims control and payment, and management reporting
OIG	Office of Inspector General's, protecting the integrity of Department of Health & Human Services programs
Predictive Analytics	Set of tools or techniques analyzing information from historical and current data to make predictions about the future outcomes or events

Process	set of activities or tasks that will accomplish a specific organizational goal
Provider	An individual who delivers health care services to beneficiaries.
State Agency	State Medicaid Agency implementing and administrating Medicaid and the State Children's Health Insurance Program (CHIP)
State PI Unit	Unit within a State Agency charged with Medicaid Program Integrity efforts
UPIC	Unified Program Integrity Contractor, will conduct Medicare, Medicaid, and Medi-Medi investigations and audits within designated geographic jurisdictions
ZPIC	Zone Program Integrity Contractor, conducting Medicare investigations and audits within designated geographic jurisdictions

ADR	Additional Document Request
ART	Audit Review Team
ATP	Audit Test Plan
DAA	Division of Auditing and Accountability
DAR	Draft Audit Report
DFO	Division of Field Operations
DFRD	Division of Fraud Research and Detection
DMIC	Division of Medicaid Integrity Contracting
EL	Engagement Letter
FAR	Final Audit Report
RDAR	Revised Draft Audit Report

1 Introduction

Healthcare costs in the United States are high. In fact, no other nation spends as much on healthcare as the United States. In 2013 healthcare spending of the US reached $2.9 trillion, equivalent to about 17.4 percent of its GDP, nearly doubling the average spending level of any other OECD country (Huffington Post, 2014).
The reason why healthcare costs in the United States continue to grow and are vastly higher than any other country is not easily explained.
However, one of the major factors contributing to such high costs and partly responsible for the current financial issues challenging America is fraud, more precisely, healthcare fraud.

In 1993, Attorney General Janes Reno declared healthcare fraud the 'number two crime problem in America after violent crime' (Sparrow, 2008). Drug dealers reportedly switched from trafficking in narcotics to defrauding the US healthcare system, discovering that doing so is safer and more lucrative while equally carried lower risk of detection and prosecution (Morris, 2009).

The implicit problem healthcare fraud carries with it, are its manifold underlying characteristics, several properties that complicate the task of 'controlling the risk'. Healthcare fraud is an intractable problem by nature. Fraudsters will find ways to defraud the system; fraud control will try to penetrate the current flaws in the system, while simultaneously the criminal effort continues to find new ways to steal money from the big pot of healthcare funds. Fraud schemes that are well designed can remain invisible for years, and thus the scope of the problem and accurate estimates of total losses remain unknown (Sparrow, 2008).

Additionally, not every dollar spent in excess is attributed to fraud. Different levels or stages of improper payments exist, and it is important to differentiate between honest mistakes being made when filling out a claim reimbursement forms at a practitioner's office, to severe acts of intentional deception and sophisticated fraud schemes to steal money, regardless of the dollar amount in question.

> *"An improper payment includes any payment that was made to an ineligible recipient, payment for non-covered services, duplicate payments, payments for services not received, and payments that are for the incorrect amount." (CMS, 2014)*

When we refer to fraud control, we imply four kinds of improper payments that create challenges for the integrity of the healthcare programs. These are:

- Error (administrative mistakes)
- Waste
- Abuse
- Fraud

They define the spectrum of fraud control in US healthcare (see Figure 1). For the purpose of this paper, we will neglect the first type, as administrative errors should not be attributed to fraud control strategies, and be addressed in efforts of educating medical providers instead.

> *"Most errors do not represent fraud. Most errors are not acts that were committed knowingly, willfully, and intentionally" (CMS, 2014).*

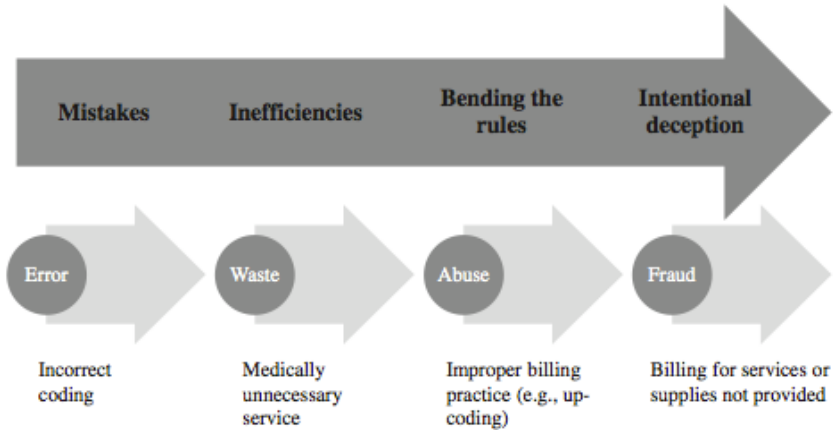

Figure 1 - Spectrum of Fraud (Agrawal et al., 2013)

Unlike errors and waste, fraudulent behaviors are usually defined as a crime in law (Joudaki et al., 2015). However, there seems to be no global consensus on the unique definition of fraud and abuse in health care services or health insurance domain.

In an effort to differentiate more distinctively between fraud and abuse, we adopt the following definitions by CMS (Medicaid Program Integrity Manual):

Fraud "an intentional deception or misrepresentation made by a person with the knowledge that the deception could result in some unauthorized benefit to himself or some other person."

Abuse "provider practices that are inconsistent with sound fiscal, business, or medical practices, and result in an unnecessary cost to the Medicaid program, or in reimbursement for services that are not medically necessary or that fail to meet professionally recognized standards for health care."

The difference between the two comes down to the person's intent to 'create' a fraudulent situation. Comparably abuse is a lesser offense, like overcharging, often associated with monetary penalties, while fraud can result in federal conviction and imprisonment.

With the exception of errors, we are interested in all types of improper payments that may be subject to fraudulent activities. In the remaining of this paper we will thus use 'healthcare fraud' to refer to fraud, waste and abuse, recognizing that these are distinct and by no means synonyms.

Regardless of type, that is, waste, abuse or fraud, all improper payments undermine the integrity and financial sustainability of healthcare programs substantially (Laursen, 2014).
Roughly $700 billion – one third of the annual amount spent on healthcare in the US - is wasted (attributable to fraud, waste and abuse); some estimated $100 billion lost due to fraudulent activity alone (Kelley, 2009).
With the passing of the Affordable Care Act (ACA) in 2010, having revised and expanded Medicaid eligibility starting in 2014, these figures are likely to increase even more.

Previous research investigating the issue of healthcare fraud in the US has focused on assessing current policies for mitigation, utilizing statistical methods or application of data mining techniques to detect anomalies in order to recover money inappropriately spent (Laursen, 2014, Thornton et al., 2014, Li et al., 2007, Joudaki et al., 2015).

Data mining techniques are particularly utilized in post-payment activities, when claim reimbursements have already passed prepayment checks and payment has been granted. Uncovered cases of fraud are then passed on to authorities who engage in appropriate actions; ranging from exclusion of providers from healthcare program eligibility, the recovery of overpayment amounts, and prosecution of all criminal parties involved.

While this may sound great, and each year the Centers for Medicare and Medicaid Services report on their Return on Investment rates, along with how many millions they have recovered due to program integrity activities, this only scratches the surface of the underlying problem. The tip of the iceberg. As Sparrow and others frequently claim, the “underlying scale of the problem remains unknown”.

Moreover, these activities are an effort to recover overpayments in healthcare expenses lost to waste and fraudulent activity that should not have been granted in the first place! Each year, investing millions in dollars for fraud control programs in order to recover a multiple of that money invested does both sound great and tragic at the same time.

Efforts must be gathered to overall assess, strengthen and control the issue of healthcare fraud. This accounts for implementing safeguards preventing improper payments to pass as legitimate claims in the first place, to identify overpayments that have illegitimately passed preventive control features, uncover fraudulent activities abusing the healthcare system followed by prosecution by law enforcement, and identification of previously unknown fraud schemes and learn from and adopt to the dynamic nature of fraudsters modifying their schemes to suit the current system.

1.1 Background of the problem

> *"Health care fraud is a type of white-collar crime that involves the filing of dishonest health care claims in order to turn a profit." (LII, 2015)*

1.1.1 Medicare, Medicaid and fraud

The United States Medicare program, eligible for persons (with legal residency of at least 5 years) 65 years of age or older, is a federally funded and administered program, providing health care coverage for nearly 50 million Americans.

Medicaid, established in 1967, is a State administered program which receives Federal matching funds and pays medically related benefits to beneficiaries. Designed as a safety-net, Medicaid is funded jointly by states and the federal government, to provide health coverage to low-income adults, children, pregnant women, elderly adults and people with disabilities (CMS, 2014). Medicaid is administered by states, which maintain their own eligibility criteria.
With the passing of the Affordable Care Act (ACA) in 2010, the total number of monthly Medicaid/CHIP beneficiary enrollment increased to 70 million as of February 2015, a 20.30% change to pre-ACA enrollment (Kaiser Family, 2015).

Together both Medicare and Medicaid thus cover about 120 million Americans, 40% of the US entire population. To express the magnitude of these two governmental health care programs, in 2013 the spending levels for Medicare and Medicaid estimated to roughly $600 billion and $450 billion, respectively. That's one third of the total healthcare spending in the US.

Healthcare costs pose one of the biggest drains on the American economy.
With healthcare spending in the US that high, there is no question as to why someone might steal from the healthcare programs. That's a big pot of money, and under millions of medical claims every year, there is good chance for fraud perpetrators to incept a few or more fraudulent claims to put some extra bills in their pockets. Among billing for more expensive services than those rendered, providing medically unnecessary services or prescribing overcharged products, up to billing for services not provided, just to name a few.

Estimates for losses due to healthcare fraud range between 3 and 10% (Travaille et al., 2011, Lorenz, 2013) of the program costs, which can easily be more than $100 billion (in words; A Hundred Billion Dollars) for all programs every year. A study by Thomson Reuters estimates up to $700 billion dollars lost due to fraud, waste and abuse annually! (PR Newswire, 2009, Kelley, 2009).

1.1.2 Technology perspective

Medicare is a federal governed body with shared information and centralized systems in place. This enables the unified effort to apply ad-hoc investigative approaches and predictive analytics in order to identify fraud, waste and abuse at

pre-payment level, or with a universal data model at historic level (Thornton et al., 2013, CMS FPS, 2014).

Medicaid, however, is managed separately by state. Each state holds sovereignty over its Medicaid program and maintains own eligibility and benefits criteria (Travaille et al., 2011). States administer their own program; thus maintaining their own information and payment systems.

Due to the variety of data models utilized by the different systems in place on state level, limited coordination across states is available. Simultaneously, the lack of unified and enforced data models makes nationwide initiatives challenging (Travaille et al., 2011, Thornton et al, 2013). While a universal data model thus allows for technological advances in fraud control with detection tools and algorithms in the Medicare domain (One Program Integrity, Fraud Prevention System), Medicaid is falling behind.

1.1.3 A natural target

Not only the billions of dollars in Medicare and Medicaid funds make healthcare fraud such a lucrative business. It is the result of the complexity and size, several structural features that make the healthcare programs so susceptible to fraud, waste and abuse (Sparrow, 2000).

The Fee-For-Service model, a payment model where medical providers are paid per service, can be seen as major enabler for medical providers to commit actions of fraudulent behavior, since they are paid for quantity of service over quality care, resulting in overutilization or overbilling.

While Managed Care, a set of techniques describing a healthcare delivery system that is ‘organized to manage cost, utilization, and quantity’, received high rates of enrollment throughout the last years, the shift of program integrity functions targeting fraud within these programs still needs to take on. A large share of Medicaid beneficiaries is now enrolled with Managed Care Organizations (MCOs). However, it has to cope with the same issues of being target of fraudulent activities daily (TruvenHealth, 2014).

Fraudsters, previously targeting Fee-For-Service enrollees by overbilling and overuse, have adapted to Managed Care by denying services to patients, providing lower quality care, or filing overstated cost reports (WSJ, 2008).

1.1.4 Fraud perpetrators and schemes in healthcare

In the healthcare domain, three major players can commit fraud. It is therefore important to differentiate between

- Provider fraud,
- Beneficiary fraud and
- Insurer fraud.

The business opportunity for medical providers is much higher (escalated in terms of economic cost impact) than those of patients (Sparrow, 2008). Li et al (2007) determined that fraud committed by providers "accounts for the greatest proportion of total health care fraud and abuse", and thus forms the 'highest risk' (Li et al, 2007, Thornton et al, 2013). The scope of this paper therefore addresses provider fraud and excludes the others.

The spectrum of different kinds of fraud and abuse schemes is large. It can be a single medical practitioner wanting to make a few extra dollars by filing for higher reimbursement rate on a single, otherwise legitimate claim. It can also be a fictitious practitioner, a criminal party buying sets of patient lists from the black-market, to steal as much money as possible charging medical services with high reimbursement rates and disappearing before any alarms sound at State, Federal or law enforcement agencies.
Sparrow (2000) identified two polar extremes in the fraud strategy spectrum:

- Hit and run
- Steal a little, all the time

There are various kinds of fraud in Medicare and Medicaid that have been uncovered so far. Although most fraud schemes may differ in scope, approach, or scrutiny, they most often can be classified according to a standardized set of fraud types.
Table 1 lists some of the most common types of fraud schemes in US Medicare and Medicaid (NAMFCU, 2015):

Table 1 - Types of Fraud

Type	Description
Phantom billing	Billing for service(s) not provided
Upcoding	Billing for service(s) with higher reimbursement rates than the service(s) provided/rendered
Double billing	Billing for same claim more than once
Unbundling	Billing for claims individually, while they should be billed as one
Bill padding	Overcharging or billing for ancillary services not needed
Kickbacks	Accepting bribery for referring patients to other providers
Identity theft	Using stolen identity information to bill for services
Fictitious practitioner	Billing for medical care without license

1.1.5 Severity and consequences of fraud in healthcare

Stealing from the healthcare program has adverse effects and there are many lives at stake. Not only can medically unnecessary services be an immediate harm to patients, but the loss of billions of dollars represents money that will not be available to provide health care services elsewhere. With Medicaid being the 'payer of last resort' and aimed for the people in need, this money is simply not available. Talking about up to $100 billion or beyond, that money could be used to provide healthcare to all uninsured US Americans (Laursen, 2014)!

Further the loss of this money is simultaneously driving up the costs of otherwise legitimate services to medical practitioners and resulting in beneficiaries being charged more for participatory costs (so called co-payments).

1.1.6 Medicare and Medicaid fraud and abuse laws

Although no precise measures of monetary amount lost every year to fraud, waste and abuse exist, over the past years the US government recognized the problem of healthcare fraud and established and enacted, or revised federal laws that govern its healthcare programs, and with it Medicare and Medicaid.
These laws specify the criminal and civil remedies the federal government can impose to fraudsters.

Federal laws governing Medicare and Medicaid fraud and abuse include, but are not limited to (Lorenz, 2013, CMS, 2014, and HHS, 2015):

• False Claims Act (FCA)
The Civil False Claims Act, originating from times of the Civil War, aims to protect the government from being 'overcharged'. That is, it poses liability to any person who knowingly submits, or causes the submission of, false or fraudulent claims to the federal government.
Together with the qui tam provision – allowing individuals to file a suit for violations of the FCA on behalf of the government – the FCA serves as the government's major tool against any individual submitting false claims. The FCA is further incentivized in that the filers (whistleblowers) are granted a defined percentage of monetary recoveries, if any.

• Anti-Kickback Statute (AKS)
The AKS defines a criminal offense to individuals or organizations who "knowingly and willfully offer, pay, solicit, or receive any remuneration directly or indirectly to induce or reward referrals of items or services reimbursable by a Federal health care program. It hence penalizes with criminal and civil action against anyone who provides kickback incentives for referrals of patients for Medicare and Medicaid services.

• Physician Self-Referral Law (Stark Law)
The Self-Referral Law prohibits physicians from making referrals for certain services to entities that have financial interest or compensation arrangements to that physician. As the name states, it aims to prevent self-referral in which the engaging actor would financially benefit twice.
Amongst additional passages incorporated in the Social Security Act and the United States Criminal Code, the Criminal Health Care Fraud Statute impose further criminal and civil actions for "knowingly and willfully executing, or attempting to, a scheme or artifice in connection with the delivery of or payment for health care benefits, items, or services to (1) defraud any health care benefit program, or (2) obtain […] any of the money or property owned by, or under the custody or control of, any health care benefit program."

Exclusions from federal health care program participation, monetary penalties, and felony convictions define actionable results of these violations.

1.1.7 HIPAA

In 1996 the US Congress enacted the Health Insurance Portability and Accountability Act, a twofold effort to protect and improve portability of healthcare information, and to ensure continuity of health insurance coverage. Title II of the act supported administrative simplification and created "programs to control fraud and abuse within the health care system" (42 US Code).
Its main purpose was set to combat fraud and waste, and to coordinate federal with state and local law enforcement. It further "stiffened the panties for commitment of health care fraud and provided the federal government with greater authority for the criminal investigation and prosecution […]" (Laursen, 2014). The Office of Inspector General claimed in its Annual Report for Fiscal Year 2013 to have "won or negotiated over $2.6 billion in health care fraud judgments and settlements" (Federal recoveries only), claiming HIPAA as the major benefit enabler for those monetary returns and success to program integrity efforts (OIG, 2014).

1.1.8 Fraud control in a hostile environment

Another feature that makes healthcare so susceptible to fraud, and differentiates from other types of controllable fraud, is defined by its setting.

Unlike other (business) domains, in the US healthcare system there is no distinctive unit being tasked with, or exclusively authorized to engage in, Fraud control activities. To make things worse, people tasked with finding fraud often do not have the necessary incentives to do so (Sparrow, 2008).

Whereas in the credit card business both the beneficiary (customer) and the credit card company have clear incentives to engage in fraud detection and prevention activities, incentives in the healthcare system are not that obvious.
A beneficiary receiving an EOB (explanation of benefits) has little reason to report to authorities if irregularities are found – assuming he or she even fully understands the mostly medical terminology and codifications on it.
In the end, the state and/or federal funds will pay the bills, often without further documentation required.

Furthermore, within the healthcare fraud control business, there is a somewhat fear towards discovering the unknown, or identification of sophisticated fraudsters, because it is harder to recover money (and efforts to do so are usually associated with high costs).
As Sparrow implied, bad news seems to not be much welcomed, as fault is usually seen by those entities that granted money in the first place.

Legislative hurdles to recover overpayments or tendencies of fraud cases to close with settlements define further features that make healthcare so vulnerable to fraud, and weakens fraud control efforts.

> *"Fraud control is a miserable business. Failure to detect fraud is bad news; finding fraud is bad news, too." (Sparrow, 2000)*

1.1.9 Fraud detection versus fraud prevention

Fraud control is a term that means different things to different people.
When we talk about fraud control, we are referring to fraud detection and fraud prevention, and define those as follows:

Fraud Detection describes activities associated with the discovery of fraudulent claims or practitioners damaging the integrity of the Medicaid program. Activities range from checks for form data anomalies, legitimacy of claims crossed with beneficiary eligibility, to medical inappropriate issuance of services through review of healthcare experts, up to conducting ad-hoc on-site audits at the practitioners office.

Fraud Prevention describes activities associated with the reduction of committed, or attempted fraud. Prevention efforts can range from legislation and policy outlines, education of medical providers, awareness of the public, and technology solutions. Law enforcement on state and federal level serves as final guardian to enforce the law to those violating these rules.

Although fraud detection and fraud prevention are distinct disciplines, overlapping activities or systems designated for each can blur boundaries of the two.

Fraud detection and fraud prevention are vital in US efforts to protecting the integrity of healthcare programs. But to what extent and effect supporting processes are deployed is not readily accessible and needs to be studied in more depth.

This section provided background information on the issue of Medicaid fraud, and highlights the need for further studies in this domain. This paper investigates both fraud detection and fraud prevention in the US Medicaid program, and studies intra- and inter-organizational processes between stakeholders involved in Medicaid fraud control. Intra-organizational refers to the activities a single party engages or is tasked with, whereas inter-organizational will look at activities between parties responsible for fraud control.
We refer to section 1.2.3 for a refined view on the research scope.

1.2 Research Design

1.2.1 Problem Statement

Health care costs in the United States almost double the costs of any other country, consuming roughly 20 percent of its GDP and still leaving 15 percent of the population (age 19 to 64) uninsured by quarter two, 2014 (Commonwealthfund, 2015). A major factor contributing to these costs is healthcare fraud, one of the biggest drains of the American economy.

While there are advances through intensified efforts in combating fraud within Medicare, Medicaid is left alone. Limited coordination efforts across states that hold sovereignty over their programs and maintain own eligibility and benefit criteria makes nationwide initiatives challenging.

States are responsible for their own prepayment monitoring with limited insight into providers history as data is maintained at state level. Data provided to CMS as overseeing entity however is post-payment (CMS FPS, 2014). This highlights the **asymmetric information between entities** that holds off efforts for better fraud detection and prevention. Even more, "efforts […] to articulate plans for the implementation of effective fraud mitigation strategies have lagged" (Laursen, 2014). Separation of jurisdiction between involved entities articulate further difficulties that must be overcome to close the gap and allow perpetrators little chance to defraud the vulnerable Medicaid program.

Thus, how effective are the controls that have been put in place to cope with the widespread problem of healthcare fraud? Do they really provide the best possible balance of efficient processes for honest medical providers, while keeping the bad guys from damaging the program? What are processes involved at entities responsible for fraud control, and how to improve such processes to mitigate fraud in Medicaid?

1.2.2 Research Objective

Although unknown in magnitude, severe damage to the economy, loss of trust in medical providers, and jeopardized healthcare quality are direct effects when control efforts within the domain of healthcare fraud prove insufficient.

The purpose of this study is to identify the actual state of how healthcare fraud is being dealt with within the Medicaid program, to shed light on those elements within the controls that are performing poor, and to propose actions formulated in models and strategies to improve detection and prevention efforts against fraudsters.
The study also aims towards the mission of the Affordable Care Act under Title VI by 'combatting health care fraud' and to "improve anti-fraud and abuse measures".

Findings of this study can be used by healthcare leaders to re-assess their own strategies as part of the Medicaid Integrity Plan. Further contribution can include the advise on implementing process improvements in the program, organizational change, and increased or re-designed technology usage.

1.2.3 Research Scope and Subject Domain

This study focuses on provider fraud, rather than beneficiary and insurer fraud. Sparrow (2008) stressed that the business opportunity and resulting economic impact of medical providers defrauding healthcare programs far out passes those of beneficiaries. We leave insurer fraud and beneficiary fraud to be the target of alternate controls or research.

The scope of this research is limited to the Medicaid program within the United States' healthcare system. When analyzing fraud control under the umbrella of healthcare, this study may discuss concepts of the Medicare program, recognizing its distinctive apparatus.

The generic part of this paper applies to the Medicaid Fee-For-Service program. Due to different settings and entities involved, generalizability to the Managed Care program cannot be guaranteed, but studied fraud control concepts may overlap.

Organizational structures, healthcare program characteristics, processes and systems may differ from those in other countries, limiting generalizability of this study towards the global healthcare industry.

Due to the complexity of fraud control in healthcare and the nature of dispersed responsibilities, policies or jurisdictive and legislative elements, certain assumptions are made that may mitigate study findings or proposed actions.

The study does not conduct evaluation of legislation or necessary policy changes, but will hint to those that pose major constraints towards proposed mitigation efforts.

1.2.4 Research Questions

In order to investigate the safeguards and processes currently deployed, and to propose improved processes and safeguards to close gaps for better fraud detection and prevention in US Medicaid, the following main question is answered:

How can intra- and inter-organizational processes and safeguards for Fraud Detection and Prevention in US Medicaid be improved?

In order to answer the main research question, the following research sub-questions arise:

1. What is the current state of Fraud Detection and Prevention in Medicaid?

We address to define the status quo of fraud control in Medicaid as of this writing; what research has been done, and what has been applied in practice?

2. What are existing safeguards controlling Medicaid?

What detection and prevention initiatives have been implemented to protect the Medicaid program from fraud, waste and abuse?

3. What intra- and inter-organizational processes are currently deployed to support these safeguards?

What activities does a claim reimbursement undergo to verify its legitimacy? What are the steps between a practitioner requesting such claim, and a possible determination of fraudulent claims, or finding of improper claims having been paid? In this part we are particularly interested in activities that occur at, but also between the parties that are being tasked with fraud control – to assess problems and opportunities for improvement.

4. What are gaps in deployed safeguards that mitigate fraud control in Medicaid?

We define gaps loosely as limitations or flaws in the control process. This could include a quantifiable inefficiency between activities, or a fundamental strategic component missing from, or governing safeguards. They can be directly associated with fraudulent claims not being caught, and therefore harming Medicaid. The extent to such will be made clear when reviewing limitations in chapter 5.

5. How can current processes and safeguards be improved to strengthen Fraud Detection and Prevention in Medicaid?

In a response to uncovering gaps we propose actions formulated in models and strategies in order to mitigate deficiencies in the control process.

Figure 2 - Research methodology

Figure 2 shows the research methodology used in this paper to systematically answer the research questions listed, the conceptual framework driving the order of this research is outlined in chapter 2.

Research question one is answered with the help of literature and document review. Question two is answered by means of document review combined with Grounded Theory, particularly open coding (Strauss et al., 1991, Saldana, 2012). Open coding allows for the identification of concepts and themes, emerging during the review of collected qualitative data. This allows us to surface the safeguards currently controlling Medicaid and answer research question two.

The third research question is answered by document review, and by the author's domain knowledge previously working as a contractor to the federal agency. Process mining will be used to determine the postpayment audit processes, following the methodological approaches by van der Aalst and Weijters (Weijters et al, 2006, Aalst, 2011).

Process mining is suited “to discover, monitor and improve real processes by extracting knowledge from event logs” (Aalst, 2011), and doing so on an actively used work system allows us to accumulate insights into how and this system is being used to find improper payments.

Despite this applicability, van der Aalst also outlined 11 challenges when dealing with process mining. C1 – the challenge of dealing with incomplete or different levels of granularity in processes – forms the one most applicable. Since we will be mostly interested in the overall completion cycle of such process, the difference in granularity may be neglected. C11 (using suitable representation to present results for correct understanding) is addressed utilizing a graphical representation of the process, and defined measure that pull the calculated values directly from the work system.

Having answered research question three and determined the AS-IS situation, question four will complete the picture by means of a gap analysis.
Research question five is then answered by proposing a set of improvements through modeling and strategy recommendations to formulate the TO-BE situation.

Semi-structured interviews using expert opinion with Subject Matter Experts (SME) validate our analysis and improvement modeling.

1.3 Document Structure

This paper is structured as follows:

Chapter 2 presents the conceptual framework that builds the foundation of this paper’s structural outline and key elements to study. Chapter 3 presents an explorative literature review on the subject domain of healthcare fraud. The literature review guides answering research question one.
Chapter 4 addresses existing safeguards and details on the processes they entail to answer research questions two and three. Chapter 5 presents the findings of current limitations in fraud control. Chapter 6 shows how processes and safeguards can be improved to reduce waste and mitigate fraudulent activities within the Medicaid program.
Chapter 7 is about validation insights through Subject Matter Expert interviews, and discussing findings in the larger context.
Chapter 8 presents conclusions to the study’s research objective and discusses limitations, delimitations and recommendations for future work.

Table 2 provides an overview of the document structure and research methodology.

Table 2 - Document and research overview

Chapter	Research question / Goal	Method
1 Introduction		
2 Conceptual framework	Definition of a baseline framework structuring problem analysis and improvement design	Preparatory Literature review
3 Literature review	#1 What is the current state of Fraud Detection and Prevention in Medicaid?	Exploratory Literature review
4 Safeguards and processes in Medicaid // AS IS	#2 What are existing safeguards controlling Medicaid? #3 What processes are currently deployed to support these safeguards?	Document review, open coding, domain experience, process mining
5 Limitations – Intra- and Inter-organizational Gaps	#4 What are intra- and inter-organizational gaps in deployed safeguards that mitigate fraud control in Medicaid?	Exploratory gap analysis, open coding
6 Improving safeguards and processes // TO BE	#5 How can intra- and inter-organizational processes and safeguards be improved to strengthen Fraud Detection and Prevention in Medicaid?	Improvement modeling
7 Validation	Re-iterate on research questions 4 and 5 Validate and discuss further insights	x2 Semi-structured SME Interview
8 Conclusion	Understanding the impact and possibilities of healthcare fraud control	

2 Conceptual framework

Having determined the problematic background of healthcare fraud in the United States, and formulated the specific research questions we want to address, we need to determine an initial framework that drives the remainder of this research.
As we are interested in assessing the current state of Medicaid fraud detection, involving the organizational spectrum, processes within and across responsible agencies and a view on the technological domain, we will apply an adaptive, descriptive version of the Integrated Organization and Technology Development framework (Wulf & Rohde, 1995) for structuring this paper.
This framework was chosen because it particularly targets the analysis of actual state at an organization, and allows providing a holistic view on improving the state by targeting the organization, process level and technology context. Other frameworks reviewed were found to not readily be applicable to the extent of our analysis, or only covered one aspect (e.g. process improvement methods, or organizational learning).

The Integrated Organization and Technology Development framework, first described by Wulf & Rohde (1995), is a balanced approach to support organizational and technological change jointly to cope with the dynamics of a flexible environment. In 1999 the OTD framework has further been applied to improve inter-organizational processes within a real-life industry context. Where the analysis of the actual state has been approached using interviews, observations and work psychological instruments, we will use the review of documents utilizing coding, domain observations and semi-structured interview to target likewise. Process mining allows us to identify the inter-organizational process during postpayment phase (where several stakeholders use one system), for which no documentation is available.

We determined that there is a need to address a broader spectrum than just the technology domain, fragmented by the structural challenges Medicaid fraud is facing. The Integrated Organization and Technology Development framework (OTD) defines such a model, which lets us address a balanced way of treating organizational, process, and technological factors within our study domain.

Although we apply a descriptive study of the OTD framework in this study, neglecting the participatory engagement of involved stakeholders, we present the idea of the framework adjusted to our research scope.

The OTD framework consists of phases, which are highlighted in the following:
The starting point of OTD, stating a problem, is defined by acknowledging our Problem Statement from the previous chapter.
The perception of the problem initiates the establishing of the process. The key player, or members of the organization that are affected by the problem, are to be engaged. The entities in the problem domain comprise of the State Medicaid agencies, the federal agency CMS, its utilization of Contractors, and the Office of the Inspector General's directed State MFCUs.

The analysis of the actual state discusses the organizational structure, processes and technology. Defining our AS-IS situation, we utilize open coding together with our domain knowledge to establish a view on current implementations.
For the post-payment review activities under the Medicaid program, we will further utilize process mining, as described by van der Aalst and Weijters (Weijters et al., 2006, Aalst, 2011), to identify and define the settings of cross-organizational processes involved. For identification of postpayment processes, we review audit trails and workflow logs of an actively used CMS system.
The creation of alternative option is a direct result from this assessment, determined by the collaborative agreement of all parties. We will utilize a gap analysis, highlighting the current organizational, process and technological shortcomings, demonstrating its critical importance to the artifact.
The TO-BE situation will again address organizational, process and technology dimensions. It will re-iterate what changes have to be made, and how they will need to be implemented to result in positive impact. This phase outlines the global concepts that CMS and leadership shall initiate to close the gaps, to phase in a better work system in order to combat fraud, waste and abuse in the Medicaid domain.

The conceptual framework is illustrated in Figure 3.

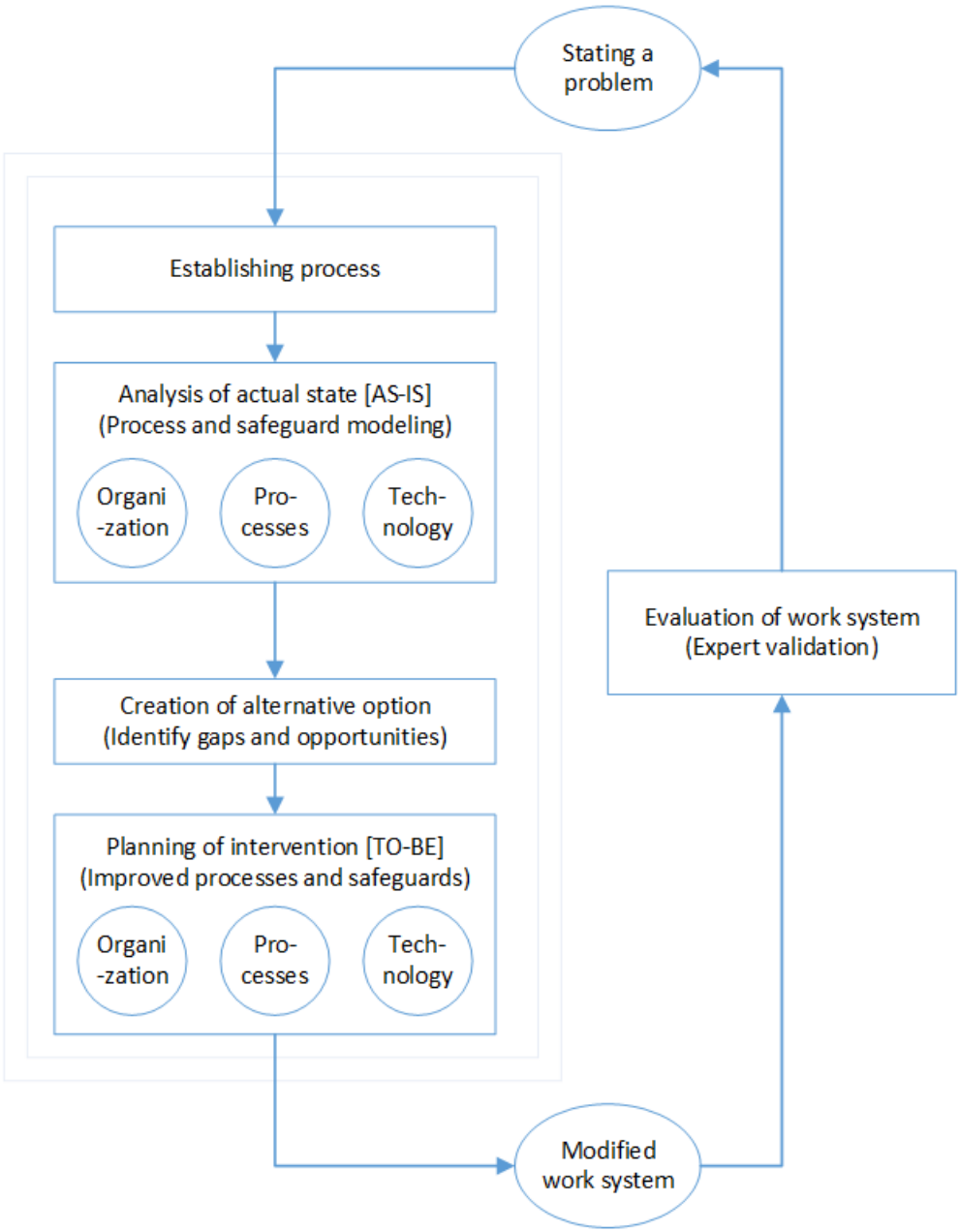

Figure 3 - Conceptual framework

We note that this framework is driving the order of this paper in its analysis of processes and safeguards that span process, technology and the organizational domain, and does not define the research methodology. Research methodology is defined in section 1.2.4.

The artifact of this paper is the described by the analysis of the AS IS situation, covering the three settings (process, technology and organization), the identification of limitations as defined earlier, and the planning of an improved situation (TO BE) outlining again key elements on process, technology and in the organizational context.

3 Literature Review

The purpose of this literature review is twofold: The first reason of engaging in an exploratory literature review is to obtain sufficient broad context information. Starting with the history and development of the US healthcare programs, focusing on Medicaid, the **understanding as to why healthcare fraud evolved into such a generic and complex problem**. The issue of healthcare fraud is not new and has attracted research worldwide. Due to healthcare fraud covering so many subject domains (medical, economical, sociological, politics and more), research showed to be manifold and diverse.
The second reason grounding this literature review is to give answer to the knowledge question as established under research question one: **What is the current state of Fraud Detection and Prevention in Medicaid?** To establish a knowledge base and answer this question, literature review was conducted in the following way:

We reviewed the academic database Scopus, utilizing search strings containing "healthcare fraud", "Medicaid fraud", and "{Medicare} OR {Medicaid} Fraud processes". Since we are interested in assessing the current state, we focused on publications from 2010 or newer, but will highlight older papers that we found to have shaped progress of academic research within this domain greatly.

For further study in this paper we also included website and document results. This was based on the belief that state of the art policies or methodologies for detecting or preventing health care fraud simply are not in one single place to find. Agencies, law enforcement and the private industry with their IT solutions offer little help in providing policies or work approaches to the general audience. Some approaches may even be proprietary or protected under confidentiality agreements. We therefore need a broader source of information, and combine this exploratory literature review with an academic search approach, while including other external sources found or linked, or providing necessary relevance to our study scope. Amongst documents included and reviewed were system guidelines, CMS program reports, publicly available reports to congress (CMS, 2014), OIG audit findings and more, found via web search. We refer to these documents in more detail in chapter 4. These documents were then examined utilizing open coding, and the emerging themes were categorized for building our analysis under chapter 4.

Pointing out the state of current research on healthcare fraud, and to point out particular lack of research in scientific literature, we present some of our findings below (we note that is not the intention of this chapter to summarize the entire state of the art of research into healthcare fraud, but to identify recent themes that have been studied, and to explore what has not been researched (profoundly)):

One older, but very important source of information describing the overall situation and challenges the US healthcare programs were and are still facing, is provided by Sparrow in his 2000 book "License to Steal" and 2008 follow up paper (Sparrow 2000, 2008). His research, offering a very in-depth study and detailed examination on the

manifold issue of healthcare fraud, served as knowledge base for a variety of research in the later years.

A comprehensive survey of statistical methods applied to the issue of health care fraud has been carried out by Li et al (2007). In their findings they claimed the need for data-driven feature selection, robust classification algorithms using noise-containing labeled data and individual methods to complement existing fraud detection mechanisms, recognizing that current tools are only moderately effective. Travaille et al (2011) further reviewed literature and assessed efforts utilizing supervised and unsupervised data mining techniques in the healthcare domain. While supervised classification may be particularly helpful in detecting sophisticated fraud schemes when factors describing these schemes are known, and training sets can be established, unsupervised techniques are needed to identify potentially new schemes and fraudulent transactions to cope with the dynamic nature of fraud perpetrators adapting to new rules and systems (Li et al., 2007, Travaille et al., 2011).

Data mining does not only include supervised and unsupervised techniques, but hybrid and semi-supervised methods. Outlier detection has been identified as a primary tool in usefulness when attempting to discover fraudulent claims in a mass of data (Thornton et al., 2013, Weng, 2008).
Bayesian methods to detecting healthcare fraud have been explored grounded by 'best cost effective option […] using mathematical models and suitable algorithms' (Elkin et al, 2013).
An IBM research in 2011 applied graphical model based methods for detecting fraud and abuse by analyzing prescription and medical claims data. Outliers exceeding certain metric are classified as candidates for further audit (Olsen et al). Further visualization studies have been approached by Copeland, applying business intelligence concepts in Medicaid (Copeland, 2012).

With the focus on the sophisticated nature of the Medicaid program, Thornton et al proposed the use of multidimensional data models and analysis techniques in order to predict likelihood and detect fraudulent activities (Thornton et al). This model was designed to cope with the issue of limited coordination and the variety of data models across states.

More recent studies explored further possibilities for applying data mining technique (Ngufor, Liu, Thornton et al., 2014), spectral analysis (Chen, Gangopadhyay) and leveraging big data analytics (in Australia) (Srinivasan, Arunasalam) to combat fraud in healthcare.
Suleiman et al recently performed a study on utilizing a data-driven approach to filter fraudulent Medicaid applications from entering the system domain, by cross-checking eligibility requirements with national databases and utilizing a scoring algorithm for each 'asset value' check (Suleiman et al).

The literature on healthcare fraud is not only limited to the technology domain. Researchers acknowledged that the issue of healthcare fraud does not fall into one

discipline, and must be tackled by activities on many levels (Sparrow 2000, Lorenz, 2013).

Areas of policies, legislation, administration and strategies for controls and leadership change have been addressed in literature.
Lorenz (2013) investigated healthcare fraud in the US, providing overviews of existing legislations and policies, and outlining strategies to further prevent future healthcare fraud. Her research spans both Medicare and Medicaid programs.
Philipps (2011) stressed the emphasis for policies under a multifaceted approach to better control and combat prescription drug abuse. She demands increased attention in the legislative arena as a critical component.
Guidance to prescriber and policymakers to combat prescription drug abuse has been provided in a Policy Position Paper by Kirschner (2013).
Laursen (2013) engaged in an explorative study investigating how health care leaders in Medicaid Arizona describe factors and needs contributing to, and necessary strategies to cope with, the issue of fraud and abuse in Medicaid.
Other papers identified focused on ethics, information non-disclosure and provider education.

Figure 4 shows the emerging themes that have contributed to research in the healthcare fraud domain, and such that targets the Medicare and Medicaid programs.

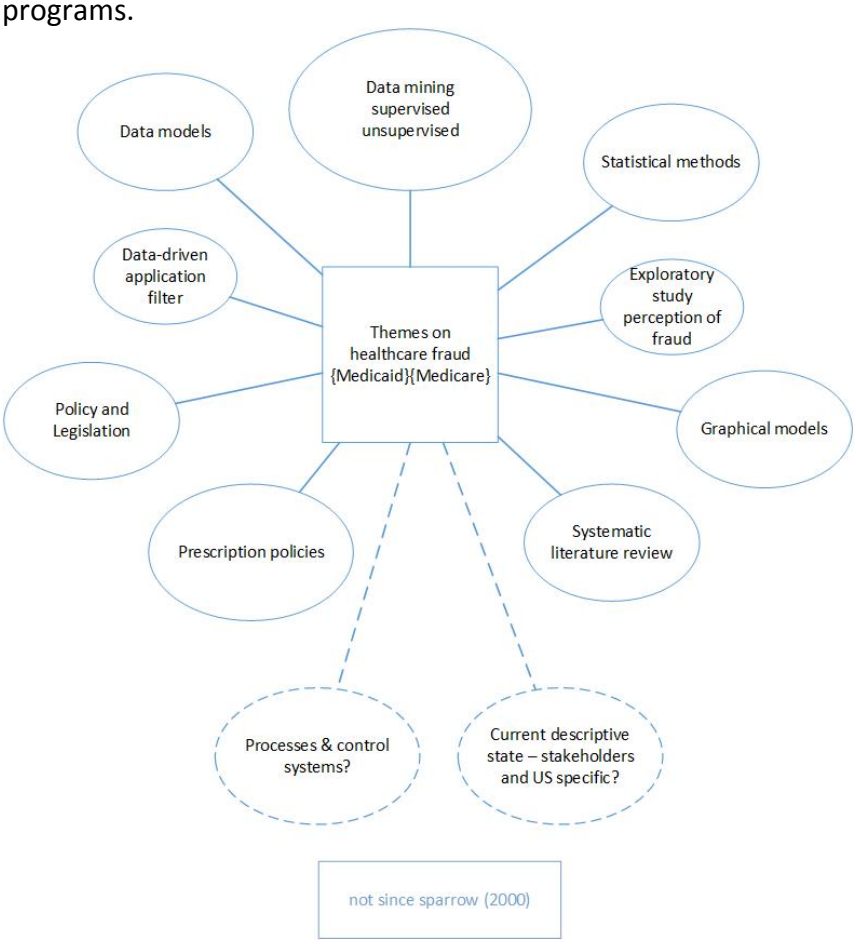

Figure 4 - Themes in literature

Reviewing the literature (study abstracts and findings) found in the subject domain of healthcare fraud within the United States, the papers reveal the following:

- (Continued) Lack of evidence about the magnitude of the problem

Although dozens of papers recognize and stress the severity of the problem, claiming estimates of millions of dollars losses due to fraud, waste and abuse yearly, no REAL measures exist. Recoveries claimed by agencies do not identify how large the problem really is, and without having a clearer picture on the amount and effect of such losses, strategies and funds to tackle healthcare fraud will continue on a small scale.

- Awareness of healthcare fraud diverging over many disciplines

The issue of healthcare fraud is not assigned to one discipline and must be tackled from multiple standpoints. Because of the complexity and size of Medicaid program, it cannot be solved by addressing the technology domain alone. Some researchers emphasize awareness of this, however, the majority of literature available is focused on the technology domain exclusively, with only a few studies exploring others.

- Under-research of electronic fraud detection (techniques)

We found many papers exploring the possibilities and applicability of data techniques to detect fraud, however, these tend to be individual approaches to detect a certain set of fraud patterns. Recognizing that there cannot be a one-approach-fits-all methodology to discover all types of fraud, more research is needed to gain knowledge on the adoption of fraud patterns, combining methodologies, and the exploration of self-learning techniques to uncover unknowns.

- Research into the issue of healthcare fraud is not much appreciated

Acknowledged by others (Sparrow, 2000, Lorenz, 2013), research into the problem and mitigation efforts of healthcare fraud is not much appreciated. Sparrow notes that professionals are interested in maintaining the status quo, since they will profit if the healthcare fraud problem remains 'invisible'. Healthcare leaders have potential reason to reject or ignore findings from research as they may questions their effectiveness or overall contribution to resolving the problem.

- Lack of research into current state descriptive study

We identified Sparrow work as a highly valuable source of information, having detailed insights into the working body of entities involved in the problem domain. Literature has since based knowledge and assumptions on this state descriptive study, and assessment from the year 2000. Research in recent years has been investigating parts of the domain, but we find a most recent assessment of the Medicaid and Medicare programs within its context to be lacking.

- Medicaid is US specific, information finding not as straightforward

This is further limited by the fact that Medicaid and its implementation is US specific, and studies within healthcare programs of other countries are not readily

transferrable. While Medicaid surely is one of the globally largest healthcare programs, Information about Medicaid needs to be aggregated and is not easily available from a single repository.

- Lack of research into processes that involve CMS and State Agencies

The literature found on Medicaid or Medicare vaguely investigates the methodologies and processes applied by the State Agencies, CMS as the Federal body and its custodians, or their use of contractors in the fraud control program.
This may be grounded by the fact that this information is not readily accessible, limited to public audience and does not fit a single discipline to have been investigated before. We are therefore also missing literature addressing the need for process improvement within Medicaid. While document reviews of reports such as yearly 'Report to Congress' point to such within the Opportunities for Improvements sections, little seems to be done using structured and documented approaches, or such information was not found to be publicly available.

This exploratory literature review allowed us to identify recent research into the domain of healthcare fraud, and those focusing on Medicaid. Acknowledging the scope of the problem of Medicaid fraud, research was found to not be complete or under-researched. We note that not academic literature was found studying the processes and controls that constitute to controlling Medicaid fraud since Sparrow (2000) has highlighted some aspects almost 15 years ago. Research may not be much appreciated, and processes and controls are not readily accessible to study; therefore we find it promising to do more research into this domain – establishing the map of controls and safeguards that stakeholders in the Medicaid domain have deployed; and to determine their effectiveness.

4 Safeguards and Processes in Medicaid // AS IS

The purpose of this chapter is to define the actual state of Medicaid safeguards and processes, as they are currently implemented and followed by all actors involved, to protect from or counteract fraudulent actions within Medicaid. This chapter is structured as follows: We will provide an overview of the four standard pieces of control systems used in Medicaid. We then engage in a more detailed view of roles of each actor involved and clarify the intra- and inter-organizational processes. We illustrate the latter by observing the process flow of a fraudulent claim reimbursement, along with a timeline perspective of the fraud control process.

The information presented in this chapter has been retrieved using the research methodology outlined in section 1.2.4.
Literature (Sparrow, 2000) and documents (CMS, 2011-2015, OIG, 2000-2014, KHPA, 2010 and others) were initially reviewed, and coding was applied to categorize existing safeguards and controls deployed in the Medicaid program. The coding, which occurred iteratively in rounds (Saldana, 2012), emerged the various controls that comprise the control domain in Medicaid based off the information reviewed. Additional domain knowledge and observations from working as contractor to the federal agency involved organized the extracted set of controls. Furthermore, process mining was used to identify the process flow of federal postpayment auditing. Informal discussion rounds (see section 7.1) were held to further structure and align the relations of identified set of control mechanisms.

4.1 Control systems

In the first years after the Medicaid program was created in 1965, only a few controls were protecting the program against fraud. However, no distinct unit was being charged with monitoring or investigating of criminal activities in the program.
Despite some early reports on fraudulent activities, it was not until the early 1970s that forced Congress to deal with Medicaid fraud on a larger scale. Congressional response to these findings was the enactment of the Medicare-Medicaid Anti-Fraud and Abuse Amendments in 1977. While this act allowed states the formation of Medicaid Fraud Control Units, it further accelerated states and federal agencies to expand and tighten their control systems protecting the Medicaid fund from fraud (NAMFCU, 2015).

Literature and documents review (Sparrow, OIG, CMS, KHPA) shows that a broad variety of control systems and safeguards emerged, each of which entails a larger subset of possible functions.
Grouping these findings led us to four key themes that are essential when talking about control systems in healthcare.

We define the following four pieces of **control systems**, each of which can be broken up further with additional safeguards and features serving a variety of **control purposes**.

Control system in US Medicaid

- Claim Processing, a.k.a. Edits and Audits
- Prepayment Medical Review, a.k.a. Manual (Claim) Review
- Postpayment Utilization Review / Cost Control Audits
- Special Investigative Units / Audits

While we identified the first named term to be of broader representation, some documents explicitly named the secondary in the domain of US healthcare. The term **Audit** further has several meanings under each system, as will be explained respectively.

4.1.1 Prepayment Review vs. Postpayment Review

In the remainder of this paper, we will refer to the first two control systems as Prepayment Review and the last two as Postpayment Review. This is supported by the fact that there is a clear break between the point of time when a claim is being processed for provider reimbursement at state level, and the point in time when claims and/or providers are being reviewed or screened, on either state or federal level for utilization review or other control forms. This break is highlighted further in the following sections.

To give a more distinctive view on the difference of prepayment and postpayment, we adopt the following definitions by CMS (CMS, 2014):

- "Prepayment review occurs when a reviewer makes a claim determination before claim payment has been made. Prepayment review always results in an "initial determination"
- "Postpayment review occurs when a reviewer makes a claim determination after the claim has been paid. Postpayment review results in either no change to the initial determination or a "revised determination", indicating that an overpayment or underpayment has occurred."

Figure 5 shows the four control systems under the two extremes, prepayment review and postpayment review.

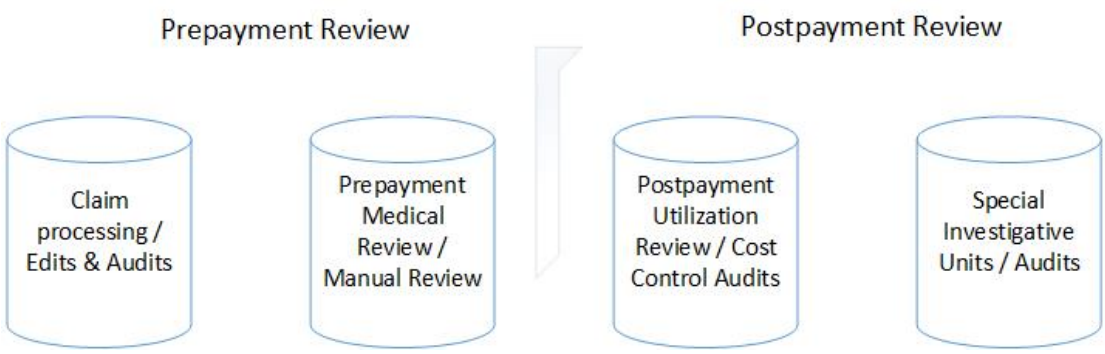

Figure 5 - Control systems in Medicaid

Next, we will describe the purpose of each of these control systems, the safeguards they entail, the way of working and their relationship to another.
This will grant us the possibility to further study their processes and henceforth to identify constraints, weaknesses or highlight issues that are crucial in efforts to reduce the possibilities to defraud the Medicaid program.

4.1.2 Claim Processing / Edits and Audits

Claims in the fee-for-service model of Medicaid are being processed at state level.
Claim processing systems are those systems operated by State Agencies to process and pay the high volume of claims submitted to states by healthcare providers.
State agencies thus operate their own electronic, heavily rule-based claims processing systems. These systems do a variety of checks and edits (adjustments), before a claim is adjudicated, that is, it is either granted payment, rejected or suspended for further, manual review.

Claims processing safeguards are those measures taken to ensure that claims submitted for payment are properly adjudicated. Processing safeguards aim to protect Medicaid systems from unauthorized access and help to ensure that proper payment for medical services is made. They may also be used to detect potentially fraudulent or abusive practices.

In order to ensure that only authorized personnel is requesting a claim, and that a claim is properly filed within reimbursements bounds, two categories of safeguards emerge: system access safeguards and claim adjudication safeguards.

System Access Safeguards
These safeguards are installed to make sure that claims are from providers enrolled in Medicaid, and prevent claims entering payment processing from those who are not enrolled, or are otherwise unauthorized to bill Medicaid.
Amongst other, the system checks for valid provider numbers, allowed third parties (billing agencies) submitting claims on behalf of providers, but also does more technical checks, like verifying whether the claims where submitted from a valid application systems and from within the US.
In addition, access safeguards may be designed to do certain pre-checks for form errors of incoming claims. For example, similar to todays most internet forms verifying whether fields are properly filled out, these checks verify if all required fields on the claim reimbursement form contain proper data. Proper data can be data that fulfills the requirement of a field (e.g. social security numbers must always consists of 9 digits), or data that can be verified as legit (SSN exists and is not fictitious).

Two types or designs of systems can be described when looking at the method of operation:

(1) Rejection upon first critical error (and no claim control number generated, OR

(2) Process claim completely until final decision is made (Include summary of errors)

The idea of the first design is, that all incoming claims are screened against proper access or form checks, and upon the first sign of incorrect data or non-legitimate usage, the claim is rejected from the system. The system attaches reasoning to the rejection of the claim and sends it back to the provider or third party the claim originates from.
No further processing takes place, no claim control number is generated in the system, and other than statistics of number of denied claims the system keeps no history of any data of such rejected claim.

The second design follows a different approach. The claim is processed entirely, including a variety of automated edits – explained below – until a final decision point has been reached by the automated system. This can be caused by any critical error found, or a threshold of non-critical errors. A summary of errors is attached, and the claim is returned to the sender. However, the system has already registered the claim and assigned a control number.

In a report from the OIG in 2010 it states, “There is insufficient information and data to determine whether one method is better than the other.”

Claim Adjudication Safeguards
If a claim has successfully passed the system access safeguards, claim adjudication safeguards take over. It is the job of such safeguards to evaluate the correctness of services billed for such as medical necessity, covered by Medicaid plan, and align with reimbursements values claimed.

Amongst those claim adjudication safeguards, Automated edit and audits, Provider flags, Procedure flags, and Concurrent reviews can be differentiated:

1) Automated edits and audits
The automated edits and audits process all sorts of data control checks on the claim. While edits generally test for data errors, the audit part runs a variety of controls or scenarios to validate if a claim meets medically necessary conditions and hence should or should not be paid. For example the audit would reveal if a service that is being billed for has policy restrictions given other claims in the patients history.
Edits are based on rule-based decision logic, coded or defined per current state Medicaid eligibility and reimbursement rates.
The edits and audits include, but are not limited to: additional form field checks, procedure code verification, provider’s checks, beneficiary checks, pricing, services limitations, check for duplicated claim and code validity.
If the edits stage fails, a similar action to the access safeguards will be taken: A summary explanation, often expressed in terms of EOB (explanation of benefits) codes – will be supplemented and the processing stops. The submitter of the claim will have to revise and submit the claim again.

2) Provider flags

Provider flags are safeguards that allow states to interrupt the automatic claim processing for a defined list of providers. The claim processing will stop and mark the claim as suspended, requiring manual review. Providers may be flagged for a variety of reasons, but ongoing investigations, repetitive improper billing, or otherwise suspicious billing behavior can lead to providers be put on such a states list.

As a direct cause, providers may have to wait longer for their claims to be processed and for payment to be granted, since manual review and additional documentation requests could easily take a few days. Because most states process payment in batches (commonly once per month), this could expand to well over a month.

In addition, states have the right to withhold payments until such suspicions are cleared.

It has however been reported that states don't favor provider flags because of adverse effects. For states these flags mean additional work, delayed claim payment, increased processing time (subject to metric), increased costs and possible litigations (OIG).

3) Procedure flags

Likewise, procedure flags can be set by states that suspend claims containing specific services billed for. This may be services that have high reimbursement rates, services that have been subject to fraudulent actions in the past, or codes that tend to conflict under certain policy combinations, to name a few. Procedure flags tend to be more common than provider flags, and states can generally adjust them.

Although we started talking in detail about claims processing **safeguards**, we need to keep in mind that this control system is only intended to constrain access to authorized parties for billing, ensure proper adjudication and auto-process a stream of provider claims.

Due to the amount of claims every state agency is dealing with on a daily basis, claims processing systems most importantly must be accurate and efficient. As an example, in fiscal year 2009, Kansas processed a total of 18.709.025 claims. That is more than 50.000 claims per day.

In addition, states are federally required to process payment for claims timely. By federal law states are required to pay 90 percent of claims – 'for which no further written or substantiation is required in order to make payment' within 30 days, and 99 percent within 90 days.

None of the safeguards discussed within this system was therefore designed to address fraud. They are simply not suited to verify a claim meeting eligibility requirements, medical appropriateness or legitimacy truthfulness reflecting actual rendered medical services to patients.

Claims processing systems are also rule-based and do not become suspicious. Their decision logic is, once a claim passes the checks, it is granted payment. If not, it is denied, or for certain rules it will be suspended for manual review.

In fact, these systems have honest providers in mind, and they do not generate fraud referrals (Sparrow, 2000).
Fraud referrals at this stage (can) only happen with human involvement. But for this to happen the claim has to get suspended first!

4.1.3 Prepayment Medical Review / Manual Claim Review

The prepayment medical review – or manual claim review – takes effect whenever a claim needs to be reviewed by specialists for proper adjudication.
This may be caused by the system suspending a claim due to provider or service flags, out of bounds reimbursements, or other defined thresholds.
State Agencies employ Medical review teams, doctors, trained specialists, nurses or other staff with proper medical knowledge, which will review the claim and may override the edit & audit actions, correct data, accept or deny the claim, or route the claim to other appropriate staff for final resolution. This process may also employ steps for comparing the claim against patients and provider historic claims (utilization) or manual pricing for specific procedure codes or out of bounds reimbursements (audits).

> *"Medical, utilization and audit reviews are claim processing safeguards that interrupt the processing of a claim for manual review by a trained specialist." (OIG)*

From general observation, four actions may be taken by the medical examiner in response to reviewing the claim:

- Approve claim
- Issue an ART - Additional Documentation Request (to support diagnosis of beneficiary, medical necessity, coverage of medical policy etc.)
- Adjust claim (based on coverage, or required judgment, e.g. for dual eligibles*)
- Deny claim (system will attach response and return back to provider)

* Dual eligibles are often subject of such reviews. Dual eligible beneficiaries qualify for both Medicare and Medicaid benefits, and two different and changing policies, may apply. Medical Review needs to determine whether services are covered, and if so, which of the two – State or Federal – is billed as the primary payer for rendered services.

Prepayment Medical Review thus is medical review judging the appropriateness of a claim or services rendered with respect to its outcome. It is a procedure designed for billing control when the claims processing system's decision logic does not suffice, or the claim falls in between decisive bounds.

Upon review, the documentation at hand – if complete – is generally seen as true unless indicating otherwise, and the reviewer makes a pay or reject decision, without any further investigative follow ups.
Any findings of exceptions or errors found by the reviewer on the other hand may be reflected back in system or policy changes.

4.1.4 Postpayment Utilization Review / Cost Control Audits

The postpayment utilization review is – as the name suggests – a safeguard that takes effect some time after the claim has been paid to the provider.
Postpayment utilization review exists for a variety of (control) purposes - like provider screening, identifying payment accuracy, identifying improper payments, identifying problematic policies or procedures, creating statistical profiles or to detect fraudulent providers - and can occur more than once.

> *"Post payment safeguards examine the accuracy of claims that have already been processed." (OIG)*

Postpayment Utilization Review is also known as Surveillance and Utilization Review System (SURS), and is utilized at two distinct stages of the fraud control process, namely at

- State Agency review and
- Federal Agency review

State Agency review happens some time after the claims were paid for any of the before mentioned reasons. States are federally required to conduct postpayment reviews, although the requirement does not prescribe defined methods or tools to use, or cap to achieve.

States, more precisely their Program Integrity (PI) units, utilize such reviews to (1) identify problematic providers, procedures or policies, (2) measure payment accuracy, (3) generate statistical profiles, and (4) to identify overpayment.
Oftentimes states have implemented such tools within their state MMIS, and SURS is being referred to as a subsystem of MMIS.

The federal agency also utilizes postpayment review, for similar as well as additional purposes.
While at state level the focus lies on internal provider profiling aimed for generating more recent insights, the federal agency has access to data of all Medicaid participating states ranging years into the past.
Such capability allows the federal agency to do all sorts statistical and data analysis, and possibly uncovers fraud, waste and abuse years after it has occurred.

Federal postpayment review however can only occur once all data has been gathered from the state agency.
Both states and federal agency utilize contractors for doing data analysis as well as auditing and recovering possible overpayments. In addition, the federal agency

evaluates all participating states on their postpayment utilization review, and requires the agencies to submit and implement corrective action plans for any error findings.

Any problem areas that emerge or outliers identified may be picked for further auditing.
Once a provider has been selected for audit, a sample of claims will be picked. The provider will be notified, and for some of the sample claims he or she may get asked for supporting documentation (ADR). If overpayment is identified, the sampling size will get extrapolated to the providers claim volume for a certain range, and the states will be charged with recovering the money from the provider.

Postpayment identifies overpayments, focusing on identifying unusual medical or billing practices (provider profiling), in order to (1) recover the overpayment and (2) educate the provider to correct their actions.

It is important to note that this control system may only be able to detect fraud with anomalous billing patterns. Otherwise it is more suited for detecting waste and abuse rather than fraud.

4.1.5 Special Investigative Units / Audits

The Special Investigative Units describe the fourth piece of control systems in US healthcare. They are responsible for investigating cases of potential fraud, stimulated by fraud referral from within any of the previous systems, or the outside world like concerned citizens, insurers or alike, and audit the parties.
The audit term used here refers to in-depth document review as well as on site studies, where a case is in the process of being formed against a prospective fraudster.
Sparrow referred to this control system sitting ‘at the end of the referral pipeline’. All instances of suspected fraud will be passed towards this unit, who take such referrals under review and form a case working with the appropriate authorities.

The Special Investigate Units under the Medicaid program are represented by the state MFCU’s, the Medicaid Fraud Control Units. We present their role and responsibilities in the next chapter.

4.1.6 Review

We have now taken a look on the four standard pieces of control system in US Medicaid. These four control systems were designed to safeguard Medicaid from improper payments.
However, as different types of improper payments exist, we need more detailed insights in the working behavior of these systems, along with roles and responsibility of people being charged with finding fraud in order to evaluate their effectiveness.
At a glance, we have also observed a first piece of control flow. That is, the systems somehow line up in sequential order: A claim will enter a state’s claims processing at

some point. If a fraudulent claim passes this system (and therefore system 2), it may still get caught by the safeguards established under system 3, and/or end up in system 4 due to fraud referral.
But are these systems enough to keep the bad guys out?

4.2 Program Oversight at State and Federal level

During introduction we have already touched upon the fact that unlike in other businesses, in the US healthcare system there is no single distinctive unit being tasked with, or exclusively authorized to engage in, Medicare or Medicaid Fraud control activities. Rather fraud control is distributed among several parties, who may be organizationally and/or physically separated.

We have repeatedly mentioned state agency and federal agency. At this stage we want to put a face on these units, organize them into an organogram, and elaborate on their roles and responsibilities participating in the Medicaid fraud control process.

4.2.1 State Medicaid Agency, CMS, OIG and MFCU

State Medicaid programs are administered by the State Medicaid Agencies, or contractors hired by those states. State Medicaid Agencies are physically located within that state, often within the states department (responsible for) healthcare services.
They are responsible for statewide administration of Medicaid related items, including enrollments, determination of eligibility and payment of Medicaid claims.

Moreover, federal Medicaid regulations require all state agencies to:

- Collect and verify basic information on providers
- Maintain a claims processing and information system (MMIS)
- Operate a SURS (Survey and Utilization Review System) (often a module in MMIS)
- Have methods for identifying and investigating suspected fraud cases
- Refer potential fraud cases to proper law enforcement

CMS and oversight of State Medicaid agencies
The federal agency administrating the Medicaid program is the Centers for Medicare and Medicaid Services, or CMS, an agency within the Department of Health and Human Services.
Formerly known as the Health Care Financing Administration (HCFA), this federal agency administers the Medicare program and, in a joint effort, Medicaid with the states.

Medicaid is jointly funded by states and the federal government, where the federal government pays a specified percentage of total program costs each year. This rate depends on the states economy and variables such as per capita income, and is adjusted every three years.

As states hold sovereignty on determining eligibility criteria (in compliance with title XIX and the ACA), but total costs are shared, the role of CMS towards the state agencies can be described as (1) actively monitoring, (2) advising, (3) supporting and (4) reviewing.
Thus CMS under the Department of Health and Human Services (HHS) holds oversight on the Medicare program, as well as jointly with the state agencies on Medicaid program responsibilities.
CMS organizes efforts and initiatives for fighting fraud, waste and abuse in both Medicare and Medicaid under their entity CPI – Centers for Program Integrity.

The Deficit Reduction Act of 2005 (DRA) significantly increased federal resources to fight Medicaid fraud. It created the Medicaid Integrity Program (MIP) – a first comprehensive federal strategy to prevent and reduce provider fraud, waste and abuse – under CPI.
The Medicaid Integrity Group (MIG) has been responsible for implementing the MIP until CMS re-organized groups and therefore responsibilities within subdivision.
CPI itself and the Investigations and Audits Group (IAG) are now responsible to

- Hire contractors to review Medicaid provider activities
- Provide effective support and assistance to states in Program Integrity matters
- Eliminate and recover improper payments

States are primarily responsible to engage in program integrity efforts and for combating fraud in their Medicaid program, while CMS provides technical assistance, guidance and oversight in these efforts.

OIG – Office of the Inspector General
Another actor participating in the fraud control process is the Office of the Inspector General. The Office of the Inspector General (OIG) is an entity part of independent agencies serving the federal government of the US.
Its existence and implementation is to conduct independent audits, inspections, evaluations, and investigations within its parent agency.
In addition the mission of the OIG is "to promote economy and efficiency and to prevent and detect waste, fraud, abuse, and mismanagement in the programs and operations of the Department and the Broadcasting Board of Governors."

The oldest and largest OIG entity was established under the Department of Health and Human Services (HHS) in 1976.

The HHS OIG's mission is defined as:

> *"to protect the integrity of the Department of Health and Human Services programs as well as the health and welfare of beneficiaries served by them."*

The HHS OIG henceforth is a distinct unit, serving, amongst others, to oversee the Medicare and Medicaid programs, although not administering them.

Administrative oversight by the HHS OIG however lies on the MFCU units. Certification, compliance assessment with statues and regulations and performance evaluation of MFCUs are responsibilities of the HSS OIG.

MFCU – Medicaid Fraud Control Unit
With the first implementation of the Medicaid program, there was no specific state or federal law enforcement agency to monitor program, the Title did not foresee safeguards in Medicaid.

The revision and enactment of the Medicare-Medicaid Anti-Fraud and Abuse Amendments in 1977 allowed states to form so-called Medicaid Fraud Control Units as a means to in fact safeguard their Medicaid program and protect the fund.
In Medicaid, MFCUs represent the control system earlier described under Special investigative Unit.

Until 1995, participation in the MFCU program has been voluntary, while federal law now requires each state to maintain a MFCU unit or submit a waiver.
As of this writing, 49 states plus Washington DC have MFCU units implemented – North Dakota holding a waiver.

> *"A single identifiable entity of state government […] that conducts a statewide program for the investigation and prosecution of health care providers that defraud the Medicaid program" (NAMFCU, 2015)*

MFCUs must be a separate identifiable unit of state government, independent of a state agency. Further, no state agency official has authority to review the MFCU units' activities.

A state's MFCU unit is staffed with attorneys, investigators, auditors and prosecutors. The idea hereby is that a MFCU operates in a 'task force approach', working year-round on cases against Medicaid fraudster.

MFCU jurisdiction is limited to the following items:

- Investigate provider fraud
- Identify overpayments
- Review complaints of resident abuse

Certain activities however are explicitly prohibited by federal regulations:

- Investigating abuse (as opposed to fraud)
- Screening/analysis (data mining)
- Recipient fraud (unless conspiracy with provider)

All state MFCUs operate under the administrative oversight of the OIG under the Department of Health and Human Services, and must be recertified annually.

Because CMS in partnership with state agencies as well as MFCUs both work in Medicaid program and to a certain extend fraud matters, the three parties frequently need to work together. The parties therefore share written agreements, also known as Memorandum of Understanding, which further outlines their unique responsibilities.

Following Sparrow, the Medicaid Fraud Control Unit is the last control system in the process, sitting at the end of the referral pipeline. Instances of suspected fraud during the process are referred to this unit, who in return investigates the matter and, if substantiated, opens up a fraud case against those parties.

Reviewing this setting and the MFCUs responsibilities constrained by its jurisdiction, this unit is largely restricted to working on incoming referrals. Since they are not authorized to engage in provider screening or utilizing similar approaches to actively target fraudsters, they (have to) rely on the stipulation at other agencies to in turn refer fraud allegations or reports of suspicious behavior, and work on substantiating these allegations instead.

MFCU units' performance is measured in terms of (open) investigations, indictments, convictions and monetary recoveries over MFCU expenditures (OIG).

4.2.2 Contractors

To complete the picture on parties involved in the US Medicaid fraud control process, one final actor needs to be introduced.
State Agencies as well as the Centers for Medicare and Medicaid Services (CMS) rely heavily upon the use of contractors (also known as fiscal intermediaries) to control fraud and abuse.

Contractors may pay claims, monitor them, target and audit medical providers; manage beneficiary inquiries and complaints. Under Medicaid – similar to Medicare – contractors run a large portion of program integrity functions.

A fiscal agent, or fiscal intermediary, is a private contractor to the state operating the state's Medicaid Management Information System (MMIS).

Under the MIP (Medicaid integrity Program) CMS is required to enter into contracts with entities in order to 'review Medicaid provider activities, audit claims, identify overpayments, and educate providers and others on Medicaid program integrity issues'.
The enactment of HIPAA further enhanced CMS authority to utilize contractors to 'ensure the integrity of the program'.

Under Medicaid, CMS is working with the following so-called Medicaid Integrity Contractors (MICs) to safeguard against fraud and abuse in the program:

- Review of Provider (ROP) MICs - analyze Medicaid claims data to identify high-risk areas, aberrant claims and potential billing vulnerabilities, and - working with the Data Analytics and Control Group - provide leads to Audit MICs of Medicaid providers to be audited
- Audit MICs - conduct post-payment audits (field and desk) of Medicaid providers to identify overpayments
- Education MICs - Utilize findings from Audit and Review MIC to work with Medicaid partners and providers, and educate Medicaid providers, beneficiaries, and others on issues related to payment integrity and quality of care

Audit MICs are the most utilized kind of contractors during CMS post-payment activities. They are tasked with the analysis of depicted medical providers, and identify any overpayments and set the path for recovering such.
Contractors may use data sets and tools provided by CMS.

Until late 2014, CMS organized their contractors for both the Medicare and Medicaid program under distinct umbrellas – like most program activities.
The Medicare contractors were organized under the Zone Program integrity Contractor entity (ZPIC), while the Medicaid Integrity Contractors under the MIC entity.
As part of a new strategy to reorganize and consolidate the work of both, CMS plans to establish the Unified Program Integrity Contractors. This would furthermore allow for increased claims data transparency, granting those contractors better insight into both program medical data to cross-analyze for improper payments and fraudulent activities.

By early 2014 CMS has discontinued contracts with Review MICs in anticipation of the UPIC strategy, and has taken over intermediary responsibility for target analysis and audit leads. CMS expects to "implement the UPIC strategy beginning with initial contract awards in FY 2015 with additional transitions to occur in subsequent fiscal years." (CMS, 2014)

Recap of organizational structure and oversight
The US Department of Health and Human Services holds administrative oversight of both CMS and the OIG. In turn, the OIG oversees the MFCU units located at state level.
State Agencies and their Program Integrity units are overseen and supported by CMS, specifically through the Centers for Program Integrity, the "focal point for all national and State-wide Medicare and Medicaid programs and CHIP integrity fraud and abuse issues".
Within CPI, the Investigations and Audit Group (IAG) is in charge to lead audits and investigations to 'prevent fraud, waste, and abuse in the Medicare and Medicaid programs'.
State, CMS and MFCUs utilize contractors for systems implementation and operation, data sharing and analytics, provider auditing and recoveries of overpayments.

Figure 6 visualizes the organizational setting of the local and federal agencies in relation to our four control systems.

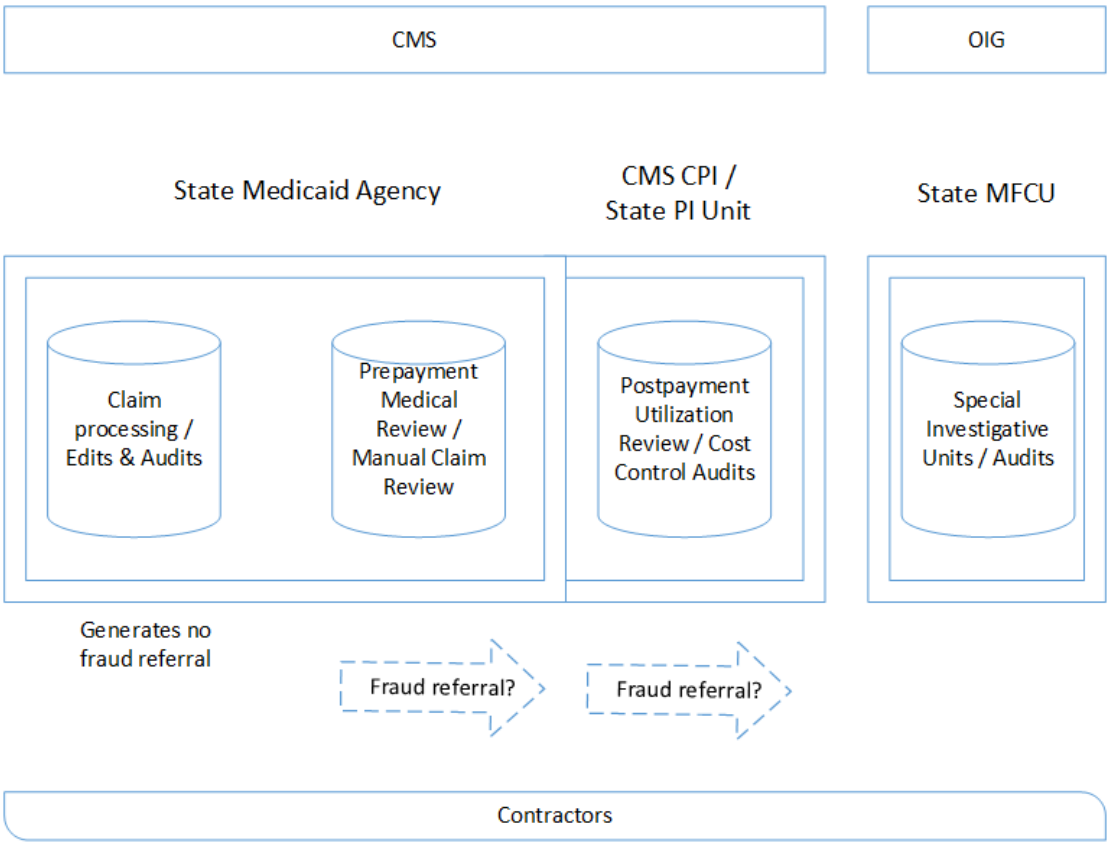

Figure 6 - Control system in organizational context

4.2.3 Review

Unlike other business domains no single unit has authority or is being charged with fighting fraud, waste and abuse in US healthcare. Fraud control in Medicaid falls under the responsibilities of several entities and actors, both organizationally and physically separated – with differing regulations or legislation.
We have introduced the State Medicaid Agency, Fiscal agents operating state systems, CMS and its units, the OIG and MFCU's as well as contractors; each of these actors participates differently in healthcare fraud control.

With that many stakeholders involved, it takes a well-structured approach, of processes, work agreements and preferably a shared vision to ensure effectiveness and properly combat fraud.
Does the intensive usage of contractors to 'source out' program integrity activities complicate the structural settings?

Understanding the responsibilities and shared participation in fraud control takes more than reviewing deployed safeguards and actors. Next we define the fraud control process, visualizing process flows for fraud control in Medicaid.

4.3 Horizontal process view – Holistic perspective

We define the following horizontal process view by observing the process flow of a claim from inception at the claims processing system at State Agency, and moving along the pipeline to federal review. We call this the fraud control process, visualized by modeling identified process flows. While the control systems order define the sequence of processes, a claim may or may not be subject to any of the three systems following the claims processing. This depends on conditions, as outlined.

The process models are a result of the previously reviewed literature and documents on safeguards in Medicaid, the associated roles of agencies and extracting relations from federal guidelines (CFR). A subset of these process flows (edits, audits and claim adjudication) was identified from the Claims, Edits, Audits, EOB Participant Guide (Ohio MITS 2010), the remainder set into context by domain knowledge and system documentation. We note that the presented process flows are a result of collecting information that was previously scattered, and – as determined by our literature review – not presented in such way before.

The Fraud Control Process

In this flowchart view, we move from state level (State Medicaid Agency and the State PI unit) to federal level (CMS and CPI, as well as contractors), with MFCU being the entity that receives referral if any of the activities throw an exception.

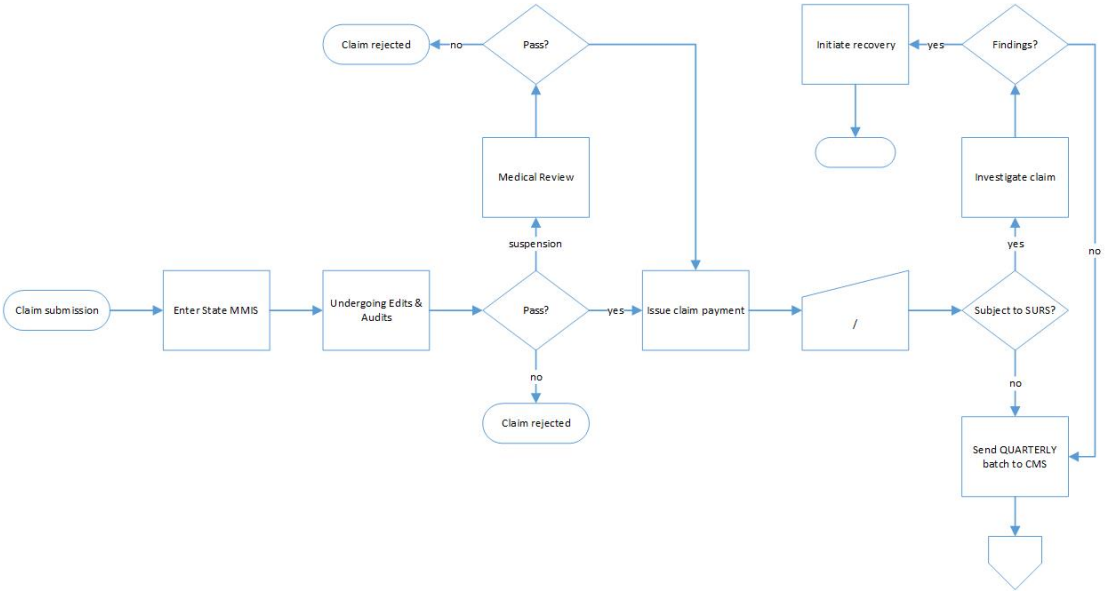

Figure 7 - Process View Prepayment (Control systems 1 and 2)

The fraud control process starts with the claim submission of a medical provider, or representative, to a state agency for reimbursement. It enters the states MMIS and henceforth undergoes a variety of edits and audits. It the claim is suspended due to failure of one or more criteria, it is put on hold for medical review. Otherwise the claim is either rejected with an explanation to its requester, or granted and put in queue for payment.

After the claim has been paid, there is no further immediate action following. The claim may be subject to state SURS review, depending on the set criteria and focus reviews. At the start of the next (fiscal) quarter, the state has to prepare the data for sending it to the state.
The process flow as part of the prepayment stage is outlined in Figure 7.

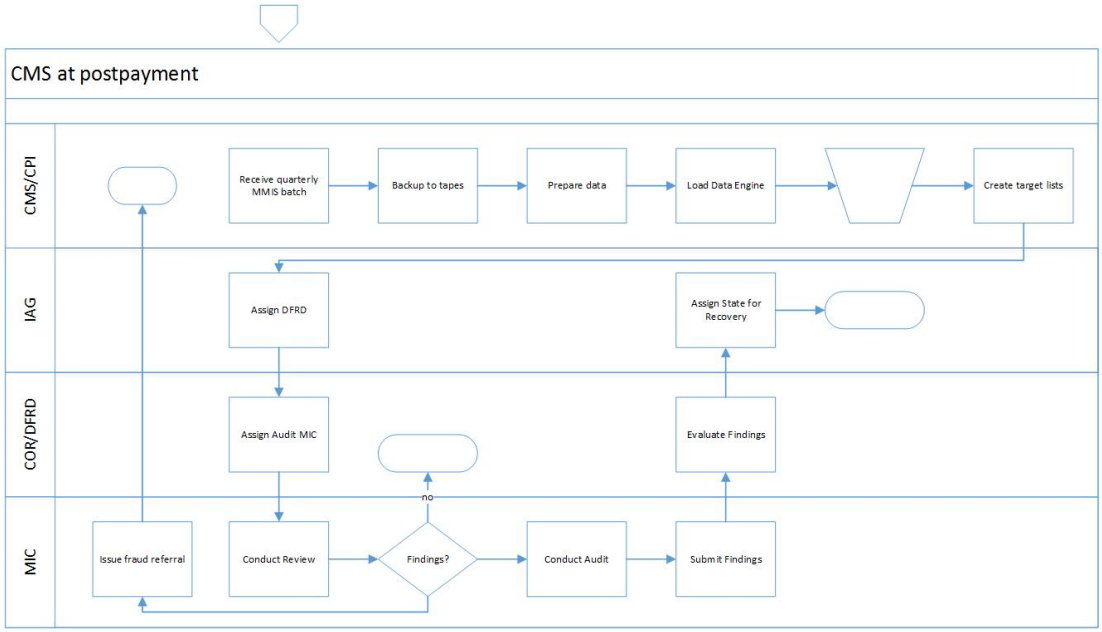

Figure 8 - Process View Postpayment (Control systems 3 and 4)

The federal side on post-payment review starts when CMS has collected (sufficient) state Medicaid data, thus when quarterly tapes with set requirements have been transferred to CMS.

CMS then backs up that data for digital preservation, as well as doing data cleansing and reformatting before further processing that data. For Medicaid, CMS currently utilizes one major tool, called the Data Engine, to idenfity and track audits, run data analyses and provide additional tools and reporting functions.

Audit contractors are then tasked with a list of potential targets of medical providers. Target lists are generated by CMS itself, or review contractors, while the responsible unit at CMS prioritizes the results for audit assignment.

Both contractors in turn may utilize datasets and tools from CMS, as well as the Data Engine, to do data analysis on historical claims for the targeted providers, and issue a preliminary result report for CMS review. Strong suspicions for fraudulent actions will result in a referral to MFCU, stopping the postpayment audit under CMS. If overpayment is identified but little indications for fraudulent behavior or patterns is found, the audit continues.

That implies that the medical providers will be notified and asked to provide documentation for a defined set of claims under review. In addition, the audit contractors may engage in on-site audits if needed.

Once the audit is completed, a final audit report is issued for CMS review as well as the provider, stating the identified findings including possible overpayments.
CMS then forwards the report to the responsible State Medicaid Agency, who is tasked with recovering the money from the medical provider within 1 year.

Figure 8 shows the process during postpayment stage.

Both models describe a holistic view of the fraud control process, staging both state agency prepayment review and federal postpayment review. In the next section, we will refine this view with more detailed processes and interactions.

4.4 Intra and Inter-Organizational Processes Refined

Having observed the fraud control process spanning the four control systems, we now want to take a refined look on the detailed actions and interactions between the actors involved. To further understand responsibilities defined we utilize a business process modeling approach, visualizing processes using BPMN, a standardized graphical representation for business processes.

4.4.1 Prepayment processes

Figure 9 shows the process flow of the claims processing control system. Once all the safeguards are passed, the claim will receive its final disposition value. If marked as ‘pay’, the claim is queued for the next batch of the fiscal agents payment to Medicaid providers.

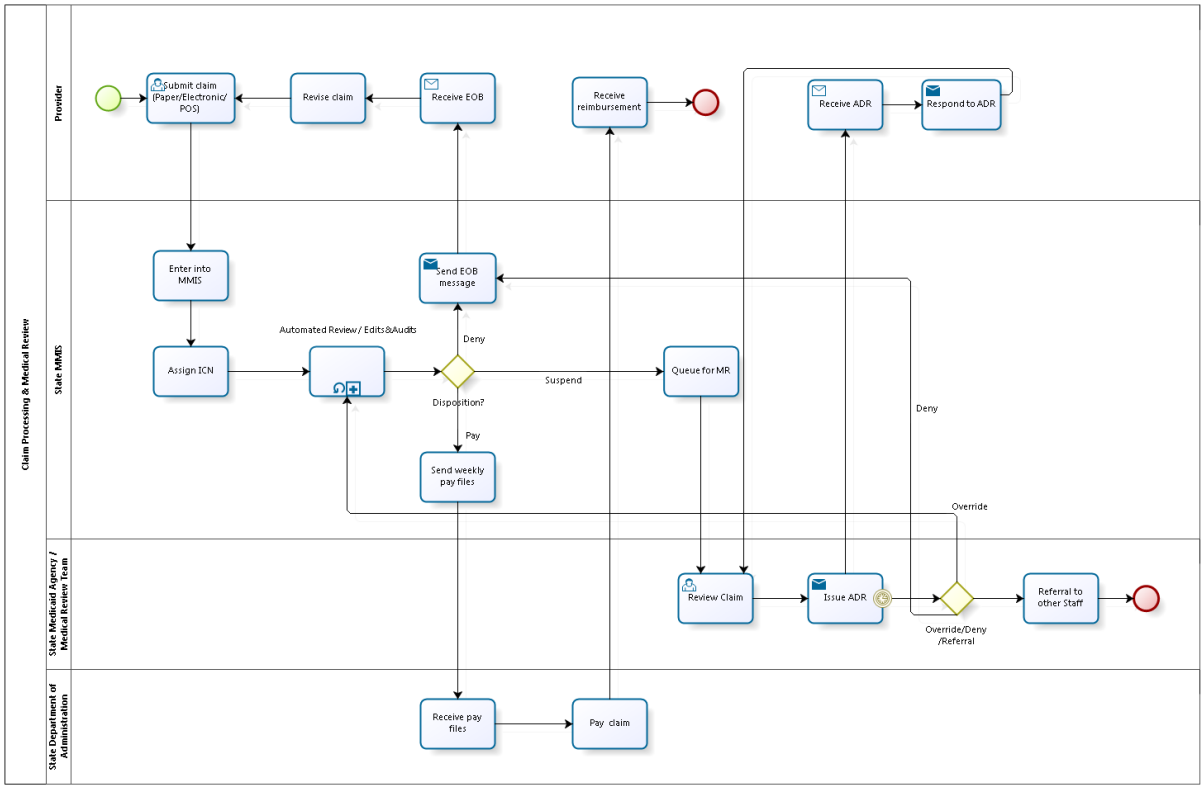

Figure 9 - Claims processing process

The observed order and interactions are highly automated. Only if the system suspends a claim it is queued for manual review and thus faces human involvement.
We further note that these system do not generate fraud referrals themselves; a claim is either accepted for payment, suspended for manual review, or rejected with a message (claim adjustment reasoning, often described in terms of standardized EOB – explanation of benefits) sent back to the requestor.

One activity in the process we need to examine further, namely the Automated Review or Edits and Audits sub-process. In this process, a variety of checks and audits validate the claim against pre-defined logic and program characteristics, to determine its final status.

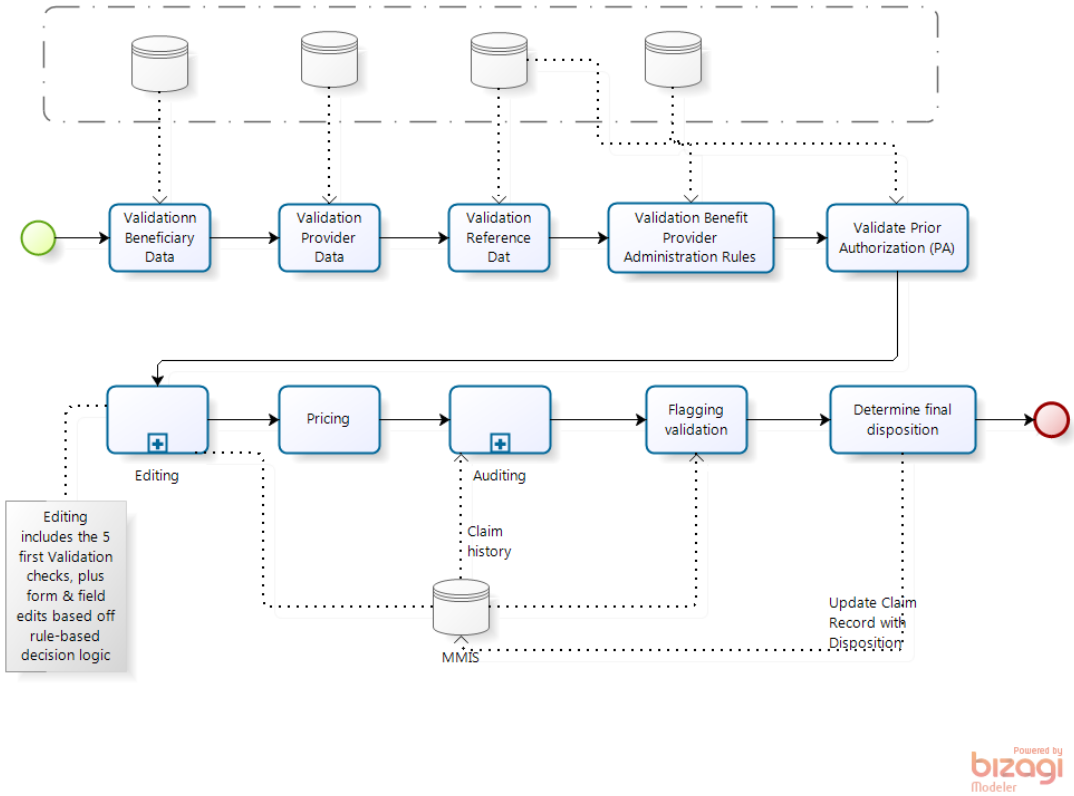

Figure 10 - Automated Review Edits & Audits

Figure 10 shows the edits & audits stage during prepayment review at state level. A variety of automated checks verify if all information is correct, and within the programs 'rulebook' so reimbursement in terms of medical appropriateness is warranted.

The edit function hereby aims to verify accuracy, validity, form format, consistency and allowed values of the data that was submitted. If an edits take action on a claim, an EOB code refers to the type of failure on the claim.
Audit checks determine if any of the services billed for are not in compliance with policies, or are subjects to certain restrictions due to historical service provisions. The edits and audits process stops by determination of a final disposition value.

4.4.2 Postpayment processes

While states collect and maintain enrollment and claim data regarding Medicaid and other state programs in their tailored MMIS, they are required to report on such data to CMS on a quarterly basis. To do so, data from the MMIS is to be converted into a national standard and submitted via secure channel Medicaid Statistical Information System. Although standardized, these data sets are considered raw data and have to be supplemented, reduced or converted once more depending on CMS' data need.

The one need we are concerned with solely is the processing of such state data for federal review:
Depending on the completeness and internal prioritization, the MIG is then responsible to send such data to the Data Engine. Again, this occurs via federally regulated secure channels. The Data Engine runs ETL logic on the received data to map and store the data homogenously in the MIG DE database.

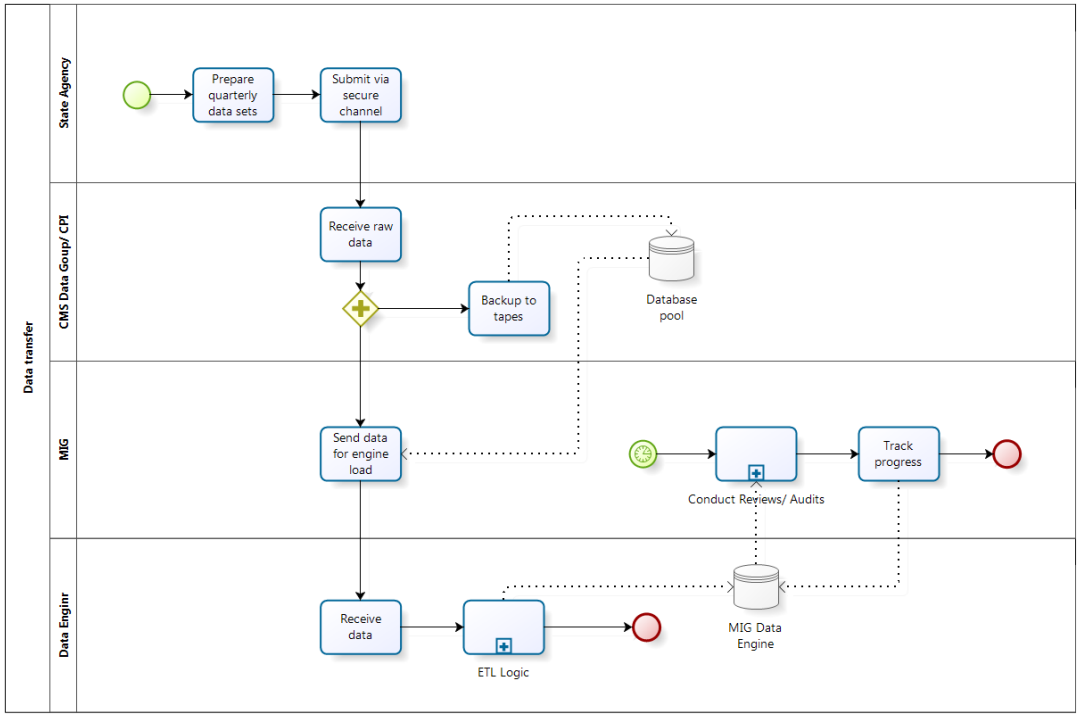

Figure 11 - Data transfer from State to Federal level

Figure 11 visualizes the described process. Once the quarterly state data are loaded into the Data Engine, they are available for CMS as well as audit contractors for further analysis.

But what exactly is this Data Engine that CMS and contractors can now utilize on enrollment and claim data to target fraud, waste and abuse in Medicaid?

The MIG Data Engine

The MIG Data Engine (DE) has been developed at the SDSC as the Medicaid Integrity Groups Cyberinfrastructure platform in response to the MIG's business needs to (1) identify medical providers who potentially have been inappropriately paid on the claims they've submitted, (2) vet that list of providers, and (3) audit the providers who remain after the vetting process to reclaim the funds paid.
The MIG DE is in operation since January 2009, and by now contains more than 10+ years of Medicaid and Medicare claims and reference data (MSIS data), totaling some 12+ TB.
Supporting a large number of users (CPI, Medicaid Integrity Contractors, CMCS, OIG, DOJ and more), the MIG DE is a clustered computational and database resource designed as a platform for analysis, data mining and interaction with this data. Phased implementation of the MIG DE has evolved a suite of data analysis, data mining, business intelligence (BI), workflow and reporting applications supporting users ranging from highly skilled analytical staff, program subject matter experts from CMS and their contractors.

Before the existence of the Workflow Management System - built to standardize and automate the MIG's ability to review Medicaid provider data, vet the results, and, where indicated, initiate and track audits – agencies and contractors handled their provider and claim analysis in a highly manual process, for example through excel spreadsheet data entries. These files were then sent around, until after at months or even years the vetting process had been concluded.

CMS and its contractor tasked with the development and support of the MIG claim a variety of success factors since inception, including an improved audit completion lifecycle by about 33% (reducing the overall audit cycle time to less than 2 years), and increased ROI rates for depicted audit types in direct comparison to previous years.

Postpayment auditing using MIG DE

CMS (CPI unit) and audit contractors (Audit MICs) utilize the MIG Data Engine to target and review sample sets of data of one or more medical providers, and to identify possible overpayments. If fraudulent patterns are observed, the audit is put on hold and a fraud referral issued.

We observe the process flow of such postpayment audit in Figure 12.

Figure 12

- removed, confidential -

- removed, confidential -

- removed, confidential -

4.5 Timeline perspective

Having studied some of the intra- and inter-organizational processes defining the fraud control process, we want to look at how these processes are dependent on time factors.
When trying to observe a fraudulent claim entering the system domain, what can we say about how long it may take until such claim is discovered? Are some of the activities constrained by regulations, system throughput, or rather the commitment of stakeholder?
It is important to align our horizontal fraud control process with a time perspective to gain further insights and nominate potential drawbacks.

As established under the claims processing system, states are required by federal law to process and pay claims in a 'timely manner'. This is further defined by requiring that 90% of all 'clean' claims (those that the system accepts without further checks required) have to be paid within 30 days, and 99% of all claims within 90 days (KHPA, HHS). In addition, State Agency systems handle claims in the amount of several hundred thousands per month, some states easily breaching the million (KMAP). Hence, prepayment processes are constrained by processing accuracy and efficiency over verification.

Postpayment processes are a bit loosely coupled, with varying duration or time spans. State Agency SURS can occur anytime after claim has been granted, however, State Program Integrity review usually concentrate their review efforts on more recent claims for statistical profiles and fiscal quarter or year measures.
When CMS gathers aggregated state data (which does happen once every quarter) proceeding timeline varies as well. Data may or may not be immediately utilized, or be loaded into further systems for analysis.
Once the data is loaded into the Data Engine, review and audits can occur anytime, but stipulated by target lists determined by CMS.
While data sets are backed up on tapes for potential future usage, the Data Engine contains more than 10+ years of available and ready to analyze.
Simultaneously, under federal laws, CMS requires providers to retain patient record for [up to] 10 years.
This allows CMS to audit a provider on claims that have been submitted nearly 10 years ago, and issue supporting documentation requests to the provider if analysis calls for further review.
Finally, the duration of a post-payment audit phase can range anywhere between months, and years to complete.
If overpayments are identified, States are being tasked with recoveries for another year. If fraud were to be found, prosecution can easily stretch this time span for another year or so.

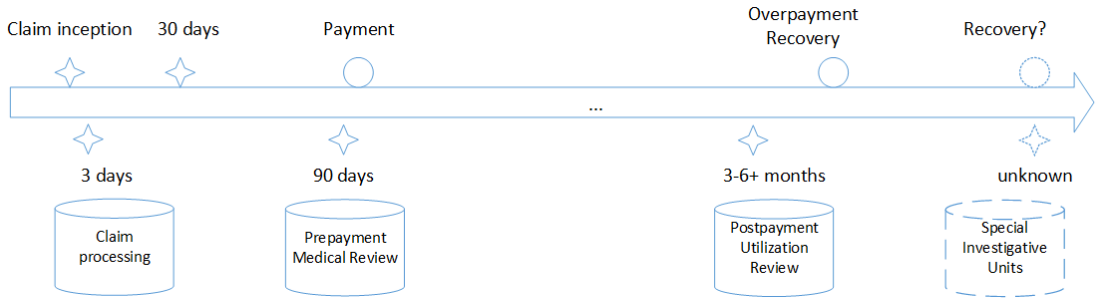

Figure 13 - The timeline of the fraud control process

When reviewing the timeline represented in Figure 13, we recall the two polar extremes Sparrow defined for the fraud strategy spectrum, 'hit and run' and 'steal a little all the time'.
While a 'hit and run' technique is riskier by nature, it appears that if fraudsters cover their claims as much as so to trick the first review systems, and claims do get paid, there is a chance they will go unnoticed for a long period of time until any sort of review or audit will take effect. That makes the latter approach a lucrative yet criminal business opportunity.

4.6 Medicaid state data and CMS data sources

As discussed, State Medicaid Agencies administrate their own Medicaid program and are required to provide system to collect and verify provider information, maintain and operate claims processing and information system (goes by MMIS), and operate a SURS.
To verify the legitimacy of enrollment information, beneficiaries and providers, states utilize a variety of data sources, for example social security records, DMV records, health plan linkages, and third party insurance resources. In turn, they maintain records of program data, provider and patient history, claim records.

For CMS to be able to engage in postpayment review, the agency needs the necessary data sets from the state agencies.
States are federally required to submit aggregated data sets, also known as MSIS data, on a quarterly basis to CMS.
Medicaid Statistical Information Statistics (MSIS) provide aggregated yet detailed sets of data on a states Medicaid program, and are used by CMS to backup for long-term storage on tapes, serve to provide information about the States' Medicaid program to CMS, and allow CMS to perform review and data analyses for a variety of purposes.

CMS State Medicaid data comprises of the following three data sources:
(1) MMIS data, (2) encounter data and (3) state program data
All three data sources are required to form complete data sets for submittal to CMS.

CMS receives the data sets, reviews the retrieved file and may request the State to re-submit if data is missing. It then backs up that data on tapes for digital

preservation, and further processes the data sets in preparation for federal review, as outlined in in the previous section.

In a response to state agencies having different sets of data formats, making it hard to suit a variety of user needs, T-MSIS (Transformed Medicaid Statistical Information System) was proposed by CMS.
T-MSIS is designed to serve as detailed national database of complete, accurate and timely data sets in Medicaid, allowing for nationwide program integrity efforts.

As of early 2013 CMS was working with 12 volunteer states on implementing T-MSIS, while other states did not started implementing, and some had no timeline to do so within their latest state Medicaid integrity plans.

4.7 Review and Discussion - Bringing the pieces together

The Centers for Medicare and Medicaid Services claims to 'apply a comprehensive strategy to prevent and reduce the potential for provider fraud, waste and abuse in the federal Medicaid program' (CMS, 2015).

We have reviewed a set of control systems that state agencies and federal agencies have jointly implemented in the Medicaid program, and studied the actors responsible for combating fraud.
By defining the fraud control process we display some of their daily tasks engaging in this matter.

Based off literature and documents reviewed, different levels of effort and commitment (in both strategy and funding) were observed. Both programs (Medicare and Medicaid) invest heavily in fraud detection and program integrity initiatives.
While state Agencies are primarily responsible for program integrity efforts and for combating fraud in their Medicaid programs, CMS aims to provide technical assistance and guidance in these efforts.

The federal agency utilizes two major postpayment review systems to systematically identify and overpayments in both programs (One Program Integrity in Medicare and the Medicaid Integrity Group Data Engine in Medicaid).

It has been found that CMS and states indeed engage in initiates for detecting Medicaid fraud, though it might be arguable whether these efforts are sufficient being aware of the (hidden) magnitude of the problem.

Fraud Prevention efforts have been increasingly addressed only in recent years, as required by passages of the Affordable Care Act (Compilation of Patient Protection and Affordable Care Act, 2010).
While the Medicare program is operating its Fraud Prevention System at Federal level for now the third year, Medicaid efforts on fraud prevention are sparse.

State agencies handle pre- and payment activities, and the federal agency only have post-payment data available. This makes nationwide prevention initiative challenging, and instead puts responsibilities for program integrity strategies down to state level (CMS FPS, 2014).

5 Gaps in current Medicaid Safeguards

On June 18, 2015 the US Department of Health and Human Services and the US Department of Justice announced the arrest of 243 individuals charged with false billings of Medicare and Medicaid programs, totaling approximately $712 million. This nationwide takedown, a combined effort of the Medicare Fraud Strike Force, CMS and law enforcement agencies, has been announced the largest in history both in terms of the number of individuals charged and the dollar amount lost (HHS, 2015).
Our analysis throughout the previous chapter gives the impression that healthcare leaders, at federal and state level, have implemented a variety of safeguards that should protect the Medicaid fund from improper payment and fraud, such as this. We now learn that by 2015 it is still possible to pull large-scale fraud schemes involving multiple states and millions $ in false billing, only to find that it took dozens of investigators in a combined effort and months of work, to announce a 'waste' in the $700 million? To make things worse, this only represents the biggest fish caught and case spread through media. It is only logical to assume that losses due to waste, fraud and abuse must be in the billions, unnoticed for years or forever.

Is the current design of fraud control not a sound approach for dealing with such a massive, high-volume, high-risk healthcare program?

In this chapter we engage in analysis to identify the problematic issues and challenges the current state of art and fraud control design is facing. We will identify such limitations, define their nature and severity, and provide ways to mitigate them in chapter 6.
We define gaps as identified limitations or flaws – that may or may not be quantifiable. Gaps could define technical challenges, lack of organizational coordination, or process inefficiencies from observed behavior.

The identification of limitations is based on our analysis of processes and agencies up to this point. Our description and review of processes, stakeholders, their relationships and information required or exchanged in chapter 4 allows us to compare the current work system against a theoretical ideal state of fraud control, and to investigate the cause of this difference. Open coding was again used on the reviewed literature and documents to identify and categorize the scattered and hidden problems. We give detail and reasoning for the choice of identified limitations in the following.

Moreover we estimate the severity of identified limitations on an ordinal scale (low, medium, high), determined by the estimated impact those gaps have allowing fraudsters to exploit currently deployed controls, and the financial impact (loss occurred) when such claims are paid. The severity assessment is evaluated during validation in chapter 7. We further split this analysis of limitations into prepayment gaps and postpayment gaps.

5.1 Prepayment gaps

1. Lack of predictive analytics or similar prevention mechanisms in place

Estimated impact: Improper payment for any sort of claims, monetary values or frequency, as long as they pass defined edits & audits.
Severity: High

Perhaps the most critical limitation in current fraud control efforts in Medicaid is the lack of (technologically supported) prevention mechanisms at State level.
How is possible that so many claims can be processed by and pass pre-payment systems, just to later be detected as billed for ineligible services or beneficiaries, duplication, incarcerated or even dead beneficiaries?

For one thing, current prepayment safeguards are designed to, and focus on claim field verification and processing efficiency. They do so, because they are handling thousands of claims on a daily basis, and are required to by law.
Thus these so to speak mammoth MMIS system, in some states implemented and operating for up to 20 years, were designed for processing accuracy and efficiency, not verification and complex analysis.

In a June 2014 report CMS claims to "be looking into predictive analytics within Medicaid", while continuing that "such likely has to be done at state level because CMS only has postpayment data available" (CMS, FPS).
While the latter is true, and states are responsible for administering their own programs including payment processing, this statement gives reason to believe that there is currently no requirement for states to have any sort of predictive mechanisms in place. In fact, under Title 42 CFR (Code of Federal Regulations) Chapter IV there is not such requirements specified. It does require Medicaid agencies to 'implement a statewide surveillance and utilization control program' which should 'safeguards against unnecessary or inappropriate use of Medicaid services and against excess payments', but does not further specify system requirements or suitable methods.

CFR and other sources show that states are required to have 'plans' established for a variety of program integrity (PI) efforts, but are very limited when talking about prevention mechanisms. Most prevention efforts focus on provider enrollment verification and provider screening, and periodic review or re-screening - to make sure only legitimate providers can bill (for) Medicaid. Regulations only require agencies to revalidate provider enrollment every 5 years – a remarkably long time considering a provider may have been alleged of wrongdoings, holds expired licenses or otherwise became illegible for Medicaid enrollment.
However, all this doesn't prevent enrolled providers from submitting fake billings, overcharges or other sort of claims that are fraudulent or otherwise improper.

When speaking of predictive analytics, one would understand a lot more than tools for provider enrollment verification. Predictive analytics often includes tools such as trend analysis, pattern recognition, detection of volume shifts or alike, all of which does not seem to be implemented when reviewing claims processing system and the automated edits & audits component in more detail.

A January 2015 report by GAO (Government Accountability Office) states that the "effectiveness of the states' use of the systems for program integrity purposes is not known. CMS does not require states to measure or report quantifiable benefits achieved as a result of using the systems […]".
Hence, even if states have components or systems for predictive analytics implemented, there are no requirements to determine their effectiveness, and the implementation and utilization of such if on a voluntary basis within states' program integrity outline.

2. Lack of Validation against other State's Beneficiary/Provider flags or federal databases

Estimated impact: Payment for providers suspended or banned in other states, for ineligible, deceased, incarcerated or otherwise illegitimate
Severity: High

This limitation has been in the focus throughout the recent years, when cases went public of Medicaid granting payments for dead individuals, inmates who should be covered by a different health program entirely, or providers that could do hit and run and 'move' from one State to another.

The fundamental issue is in the nature of State Medicaid agencies administering their own programs. Because states have different eligibility criteria, but also technically different systems and are physically located disperse (namely in each state), there is no cross-collaboration happening with other states.
CMS provides technical assistance to states, but no centralized data marts are accessible, and states need to maintain records utilized for claims processing up to date themselves. This includes beneficiary information and social security records.

Information sharing between State Agencies or MFCU units is a manual process, and a state agency reviewing a provider enrollment does not immediately know if that provider happens to be or have been registered in another state. There is no national healthcare provider database states can access for provider enrollment. Other databases that exist and CMS requires states to be checking their records against suffer from usability (List of Excluded Individual/Entities (LEIE) only allows a small number of names or SSN to be searched for), purpose (Excluded Parties List System (EPLS) containing excluded contractors, or outdated information (Social Security Administration Death Master file).

Even more severe seems the fact that CMS does not have a system in place where states can access to determine (temporary) Medicaid provider suspensions in other states.
In 2011, per requirement of the Affordable Care Act, CMS contracted out the development and started operating the 'Medicaid and Children's Health Insurance Program State Information Sharing System'.
Despite its promising name the system failed almost entirely, based on an OIG audit conducted March 2014.
It was claimed that the system 'fell short' because of a variety of reasons, most prevalent:

- States were not entering information; for several states the system did not contain any entries at all
- False or incomplete information; while the database was meant to track terminated or suspended providers, some of the entries reflected providers that were dead, retired or did not longer participate in (a state's) Medicaid program
- Moreover, a significant share of the entries did not contain a so-called unique provider ID, making State Agencies queries almost useless.

One of the more interesting pieces of information the audit revealed however was the fact that for the past 3 years of its implementation, CMS did not require states to report to the system at all, although they would have the 'power to do so'.
As of mid 2015, a new initiate for a provider tracking system was planned, and request for proposal issued (McKnight, 2015).

3. Low Utilization of States' Medical Review / Fraud Awareness

Estimated Impact: Payment for claims that could easily be questioned by a reviewer, full-payment of claims that could have been adjusted prior, losses due to not adjusting work systems
Severity: Medium

As we have shown in our analysis of prepayment processes, the States' Medical Review – or Manual Claim Review – is dependent on the MMIS systems' determination of edit & audit checks. In fact, unless the system suspends due to one or more pre-determined logics, no 'clean' claims will ever go under Manual Review.
The system is not designed to detect un-programmed anomalies, and does not become suspicious.
Reversely, all claims that pass the edits & audits stage are assumed to be valid (for the time being), and the system itself is not tested against possible weaknesses.

It requires the postpayment review, at either State or Federal level to uncover fraudulent claims, and only after doing so the States' claims processing system may be adjusted to detect such fraudulent claims or larger schemes.

While the Medical Review procedure may be designed for billing control rather than claim validation, it defines the last pieces of control before a claim is accepted for payment and possible erroneous payments are granted.

As we have indicated possible reluctance of State Agencies to suspend payments to providers, the CMS June 2014 report reveals further issues with this strategy.
Despite revised federal regulation in 2011, some states do not suspend payments claiming reasoning of missing state authority, missing documentation to support doing so, or the verbal request of the MFCU to in fact NOT suspend payments.

If Medicaid Agencies do engage in Manual Review, further problem arise with the identification of fraud and to convert these insights into preventive measures.
Rather, Medical Review is a game of negotiating the prices with the providers (if system suspends to due exceeding thresholds), or educating them or their assistants for proper billing.
The single review of a claim along with supporting documentation leaves little room for Medical Review team to form an actual fraud suspicion. Reversely, if no or illegitimate documentation is returned, only then the provider may get 'flagged' for additional reviews.

42 CFR § 455.23 regulates the 'suspension of payments in cases of fraud' for Medicaid Agencies. It prescribes the suspension and reporting requirement for credible allegations, but it is up to the agency to determine such.
It is a question of how fraud aware the state agencies in fact are, and if they are sufficiently trained towards identification of fraudulent behavior or billing pattern. If no measures exist that evaluates suspension and referral rates from Medicaid agencies, little incentives are put in place for Manual Review to engage in fraud control.
The Medical Review under the State Agency can therefore be described as to act in re-active mode, evaluating medial appropriateness over formulating fraud suspicion.

Ultimately, the failure of this control system leads to the fact that fraudsters are and cannot be caught on time (that is, until payment is granted and the damage has occurred), new schemes or behavior are not learned and fraud awareness maintains at low level, as well as the prepayment system (state MMIS) is not revised and maintained timely to cope with the evolving nature of fraud or entire schemes – adjustments that could quickly be made if only one fraudulent provider is studied during medical review.

5.3 Post-payment gaps

1. Delayed / Halt of data loads for CMS postpayment review

Estimated impact: Postpayment audits only on claim and MSIS data before mid 2014.
Severity: High

At the time of this research the MIG DE still is the only federal centralized data system used for nationwide and possible cross-state data analysis, and similar tools to run and track audits on Medicaid providers.
However, as of mid 2014 CMS has stopped loading data sets into the Data Engine, presumably in anticipation of the upcoming unified data system covering both Medicare and Medicaid, and related strategic and business reasons.

Since the halt of data load, CMS and contractors can now only run postpayment audits on claims and MSIS data up to mid 2014. To make things worse, several of these states' data sets are even older than the mid 2014 point in time.

This limitation entails a severe impact;
It implies that, in theory, any Medicaid fraud committed since mid 2014 - that has been granted payment and has not been caught by states' postpayment review – can only be uncovered if the new data engine is deployed and all data sets are loaded to be accessed (!).

While we can expect that large sets of data will be made available upon deployment, the ongoing slow progress of implementing T-MSIS poses another limitation.
By March 2015 the progress for T-MSIS has been claimed as not completed, and it unclear when it will be.
Although CMS has authority to "withhold Federal matching payments for the use, maintenance, or modification of automated data systems from States that fail to report required data", it would seem unwise to cut matching funds at a point where CMS wants states to focus on.

2. Postpayment auditing inefficiency utilizing DE

Estimated impact: Poor efficiency in recovering overpayments or detecting fraud
Severity: Medium

Following the delayed and as of mid 2014 stop of data loads into the Data Engine, our review also noticed a variety of inefficiencies in utilizing the MIG DE.
First, postpayment audits for recovering overpayments take a remarkable long time to be completed. While it was claimed that the deployment of the MIG DE has decreased the average audit completion lifecycle by 33% because of automating processes that had previously been done manually and using hard copy files, the

average duration of audits now between 12 and 24 months still takes a considerable long time to complete.

In addition it appears that the audits are targeting the same provider types over and over again. With the general hospital and hospice holding a share of almost 60% of all audits, it almost seems that the joint practice from next door will not be targeted by postpayment review. One could argue that these provider types are targeted for having a potential of larger overpayments than smaller practices, or it might even be easier to reclaim money here. However, federal audits are digging in the same holes they have been successful in before, not the ones that might actually be fraudulent.

Another limitation identified includes the lack of implemented metrics to evaluate contractor performance. While the Data Engine supports Business Intelligence reporting to define metrics for a variety of business needs, is has not been utilized by CMS to track the performance of their contractors. Contractors are essentially competing with identifying overpayments within their assigned region, but without CMS being able to review such performance, the full potential remains unleashed.

Finally we want to evaluate the recovery amount of completed audits.
In 566 audits that have been completed (and Final Audit Reports have been sent to State for recoveries), a total of 81.5 million can be claimed.
With the MIG DE project costing around 35+ million since its inception in 2009, we could calculate a ROI of a little over 2 to 1. However, technically speaking the MIG DE entails more than just the workflow application despite this being most utilized tool. A return on investment of 2 to 1 might be justifiable because recoveries still amount to millions in the two digits area, but considering reported ROI in other program integrity initiatives this is not an impressive number – and again only scratches the surface of the underlying problem.
Because of the recent shut down on utilizing the DE to perform audits in favor of the upcoming unified approach these identified inefficiencies might not be considered to be relevant any longer, however, without a careful assessment of such the new approach is likely to suffer from the same or similar limitations.
These insights should be carried over into the upcoming system by reviewing procedures and process flows, preferably during development of the system.

3. Passive role of MFCU / Who actively seeks fraud?

Estimated impact:	Lack of coordinated control strategy reduced potential of fraud detection
Severity:	Medium

Although we have not studied the processes for MFCUs in much detail, we can evaluate their role in the fraud control process.
From its jurisdiction we outlined earlier and its setting in the process pipeline, the MFCU can best be described to be in reactive mode.

MFCUs are tasked with investigating fraud upon request, either by referral from State Agencies, concerned citizens or alike. These units take on alleged cases of fraud, and investigate to harden or possibly dismiss the case. We have also noted that MFCUs are evaluated in terms of investigations opened, cases closed and recoveries claimed. Now, if MFCUs are allowed to only investigate provider fraud, and to that extend also rely on referrals for doing so, then what other entity is being tasked with active lookout, screening and identification of fraud at beneficiaries, providers and possibly insurers?
While CMS – having only postpayment data available - engages in identifying overpayments using audit contractors, they rely on its contractors to formulate allegations of fraud during their review.

State Program Integrity (PI) units are tasked with fighting fraud in their programs, but how effective are these units in this effort? And if its sole responsibility of PI units for detecting fraudulent claims, or entire fraud schemes, then how are they evaluated? What about if they don't find anything? Are they held accountable?
Through the Improper Payments Information Act (IPIA) enacted in 2002, CMS as the federal agency is required to annually review programs they administer, and to identify and report on those that may be susceptible to improper payments (CMS).
Under Medicaid, the Payment Error Rate Measurement (PERM) had been introduced. On a 3-year cycle (takes about 26 months to complete a PERM measurement) states are evaluated and as such, the State Medicaid agency and its PI efforts are being reviewed. Upon findings and identified errors, as well as any overpayments identified from studied samples, the states have 90 days to submit so-called Corrective Action Plans (CAP) back to CMS, and initiate recovering overpayments and to return federal share to CMS. Noting that PERM is not a pure 'fraud rate' but a measurement of payments that have been made which 'did not meet statutory, regulatory or administrative requirements'.
With the PERM rate and its purpose in in mind, CMS seems to be doing very little to 'enforce' commitment for PI units, but rather 'evaluate' state agencies by exercising program integrity reviews, and determine non-compliance along with requesting agencies to implement corrections.
We note that, while CMS has the authority to withhold payments if statutory or regulatory requirements are not met, they simultaneously rely on and need the state agencies and their efforts in combating fraud – which in turn depend on the federal share of financing.

4. Ongoing organizational and technical challenges at CMS

Estimated impact: Missed opportunities and slow adoption of fraud control improvements
Severity: Medium

CMS started a large re-organization in late 2014, and, as of this writing, was still in progress of completing such.

The Medicare and Medicaid program integrity efforts will be merged on a variety of matters, including administration and tasking of contractors. The Unified Program Integrity Contractors will replace the MICs, and ZPICs in Medicare.
Although MICs have not yet been cancelled, it may be questionable whether their performance is still being tracked for. As we have shown under postpayment auditing, appropriate performance measures have not been implemented by CMS to track auditor efficiency. No evaluation can be made if CMS and other healthcare leaders have acknowledged this, and will do implement such when utilizing UPICs.

While the new data engine and auditing system for CMS is still under development, utilization of legacy systems is being shut down. We note this to be particularly risky as the new system and tools likely will not be available or fully utilized within the next several months. Meanwhile, the Medicaid in particular is in risk of being defrauded while appropriate countermeasure cannot be taken.
The ongoing implementation of T-MSIS for now more than three years, and CMS' reluctance to apply statutory enforcement by withholding payments (for either data systems or medial assistance for managed care enrollees) or similar poses another opportunity that could have been taken advantage of by now.

5.4 Discussion & Review

We have presented an overview of the fraud control process, and safeguards governing the Medicaid program. In this chapter, we show how the current process has a number of limitations, and therefore cannot potentially live up to be sufficiently safeguarding the Medicaid fund from fraud, waste and abuse.
Prepayment and postpayment controls lack organizational harmonization, while missing opportunities coin the technology perspective.
Whereas in Medicare CMS claimed its second implementation year of the Fraud Prevention System (FPS) announcing a 5 to 1 ROI for Fiscal Year 2013 with over $210 million recovered, Medicaid is lacking essential prevention mechanisms. CMS' Data Engine for protecting the Medicaid fund can barely be called a success.

Medicaid is also known as the payer of last resort!
This implies that payment should only be granted if all other healthcare options are scooped. It is therefore of great importance that state agencies only process claims that fall under current program coverage using sophisticated pre-checks.
This however does not entail checking claims of its validity.

Sparrow (2000) determined that *"the predominant forms of fraud […] consist of overprovision of services based on false or exaggerated diagnoses, and billing for services that were not actually provided."* With millions of dollars identified in just a number of audits, too much is to be identified during postpayment review as improper overpayment, money that should not be paid in the first place.
While current measures cannot clarify how much is, or has been successfully prevented as part of PI efforts, it seems obvious from our analysis that – in its current

state of implementation – Medicaid fraud control focuses on postpayment review over prepayment validation.
There appears to be a somewhat 'fuzziness' of lines between fraud, abuse, waste, and overutilization. The bar might be set high as to what qualifies fraud, and even if allegations exist, it is hard to actually proof fraud. Manual review – a stage that has the expertise in the form of staff members and supporting documentation focuses on medical appropriateness and pricing rather than look for fraud. Even if improper payments are found, there appears to be a reluctance to charge and disqualify, and rather engage in settlements by claiming the money back.

Finally, we are concerned with the lack of accountability for fraud in Medicaid. Whether fraud is found or not, no entity is being targeted directly for failure in their control. If fraud referrals are issued, MFCUs are tasked with forming a case, if fraud during postpayment is identified; CMS works directly with MFCU and prosecutors to charge the ones responsible. The identification of overpayment and therefore un-classification of fraud is sent to the state being tasked to recover the money.
No entity appears to be held accountable for money wasted in the first place, not entirely surprising if almost no metrics exist or are implemented.

6 Improving Processes and Safeguards // TO BE

The deployment of safeguards as a means of protecting the Medicaid fund is, without a doubt, an essential key asset to have in place. We have shown that these tools however appear to be little effective in identifying or preventing improper payments, and fraudsters still have easy game when targeting Medicaid.

In this chapter, we address the limitations that we have identified in the fraud control process and provide suggestions for improving the process or properties of safeguards to overcome the lack of control and inefficiencies found. Because one approach might be closely coupled with another, it becomes harder to differentiate prepayment from post payment safeguards and vice versa within this chapter. We therefore shift towards linking our recommendation to the process, organizational and technological perspective, as outlined by our framework.

A holistic view in combination with our framework allows us to understand and consider the organization as a whole. We want to suggest and if applicable model improvements, and it is therefore necessary to look at the various connections that define the current setting in fraud control. Improving a single process (e.g. contractor throughput) does not contribute to improved fraud detection if the other stakeholders contributing to the process cannot keep up with the review and approval of findings. To increase the organizational capability on multiple levels – we review technical, process and organizational aspects to provide recommendations that have an impact in one or more levels at a time.
The holistic view therefore allows us to formulate a set of alternative options in a response to our identified gaps, to build a TO-BE situation for better controlling Medicaid fraud.
The generated recommendations for actions are in turn highly conceptual targeting a variety of change requirements, and as such need more research into their technical and political feasibility. However, a holistic view provides us with a clear overview of the changes that are needed to define impact that improves fraud detection or prevention, as outlined in the following.

6.1 Prepayment safeguards

Technological view

1. **Require State Agencies to implement Predictive Analytics**

State Agencies are the first line of defense in Medicaid fraud, without a doubt. Therefore, healthcare leaders including CMS as the overseeing entity need to ensure that states have access to and operate most up to date information system.
Some of the states MMIS systems have been deployed years ago, unable to supply critical tools that allow for prevention mechanisms as todays systems can offer.
They do not become suspicious, they do not allow for trend analysis, pattern recognition, and detection of sudden volume shifts or alike.

As part of this effort, State agencies should be further be required to review and revise their systems for

- Beneficiary Medicaid applications
- Provider enrollment and re-enrollment/re-evaluation

to filter fraudulent or otherwise illegible applications and submissions.
Regarding the first, Suleiman et al also acknowledged the lack of attention in IT support for detecting fraudulent Medicaid applications, and proposed a 'data driven implementation using a layered architecture to filter' such fraudulent claims (Suleiman et al., 2014).

The federal regulation requiring states to revalidate providers enrollment in their program *only* every 5 years should also be re-assessed, and preferably tightened to ensure only legitimate and eligible providers continued to be enrolled (CFR).

Potential for validation of beneficiary and provider data against other states data should be explored, which is further reviewed in the next section.

One critical item to support and in fact enforce the State Agencies to modernize their technological toolset is the CFR and its regulations under title 42 Public Health.
The CFR currently only requires the implementation and operation of a program integrity program 'control program', and further requires that State Agencies have methods in place to implement such control, but it fails to define more specific regulations or types of technology supported systems that must be utilized.

CMS is further authorized to provide matching funds (to cover up to 90 percent) to assist states in their efforts of implementing and operating systems to support administration of their Medicaid programs – including program integrity – but states need to establish plans and actually request those funds.

Additional lack of metrics available for CMS, and the not existing requirements for state agencies to report on the efficiency of their program integrity controls, makes it even harder to evaluate effectiveness and progress of today's implementation at state level.

Specific actions to be taken therefore should cover:

- Revision of CFR Title 42 - Chapter IV - with a focus on prevention efforts and utilization of prediction tools
- Metrics need to be introduced, for both CMS to compare all states agency administration and PI efforts, and for states to report on their utilization
- Funds need to be made available for implementation of tools and systems (they already are), and states need to be incentivized to claim these funds

Along with ways of incentivizing, how to make it a requirement for states to invest in new PI tools? It should be the joint goal in keeping the States' array of tools and methods up to date, and not take actions if systems fail or regulations finally dictate they must. This could either be looked at as a top-down approach, regulated by

healthcare leaders, or a collaboration of CMS working with states. However, more stringent guidelines are necessary.

Process and Technology view

2. Implement ways for cross-state validation of Beneficiary/Provider flags

At the time of this research, State Agencies are almost entirely isolated when it comes down to verification of a provider enrollment, and their MMIS system running the edits & audits checks.
In order to prevent payments for providers that are suspended or potentially banned in other states, or flagged beneficiary IDs or otherwise determined as nationwide ineligible, a federal initiate needs to be started. CMS has previously failed with an approach targeting this issue.

One option would be the installation of a federal data-sharing system to keep track of states' banned, terminated, or currently suspended practitioners.

By drawing lessons from an earlier approach (Medicaid and Children's Health Insurance Program State Information Sharing System), CMS will need to *require* states to

- Provide data on provider suspensions or terminations to the system in a timely manner
- Conform to he outlined requirement of providing all necessary data to ensure entries are clean and complete
- Validate their own MMIS records against system periodically, and take action and response for any findings

An alternative, and rather radical approach could be to target the separated nature of prepayment Medicaid systems. We recall that CMS has only postpayment information available, and even the State Agencies are almost entire separated from the knowledge and data pertaining to other states' Medicaid program. With the assumption that the Medicaid program will continue to be administered at state level, CMS and healthcare leaders should seek opportunities to integrate (parts of) these separated controls.

The implementation of a hub-and-spoke architecture could potentially satisfy this business need and enforce data transparency amongst prepayment review level in an approach to integrate state MMIS implementations.
Federal level would be designated to establish the hub and determine the data that is to be shared, in particular beneficiary, provider and insurer level data, state provider and service flags and their reasoning, along with other high profile data that is deemed valuable for further prepayment analysis at state level.

One of the benefits would include that State Agencies could maintain their applications, and only have to establish the connectors to the hub. Similar to their

current requirement for becoming T-MSIS data implementation ready, they need to be mandated to contribute as well as utilize data from the hub during prepayment processing. CMS has authority and likely funds available to support states in doing so.
Downsides of this approach include concerns of scalability and control of such a large-scale project involving 50 states, and project costs ranging into the hundreds of million dollars. Once completed, the benefits of supporting prevention efforts nationwide however can be significant, yet hard to estimate.

Medicaid is a national program (yet administered by state) – thus a FEDERAL initiative should be sought and be in everyone's best interest. An approach like this can be considered durable when states maintain administrative oversight and eligibility criteria on their programs.

Figure 14 shows how a federal initiative could lead the way for states to cross-validate prepayment data against other states.

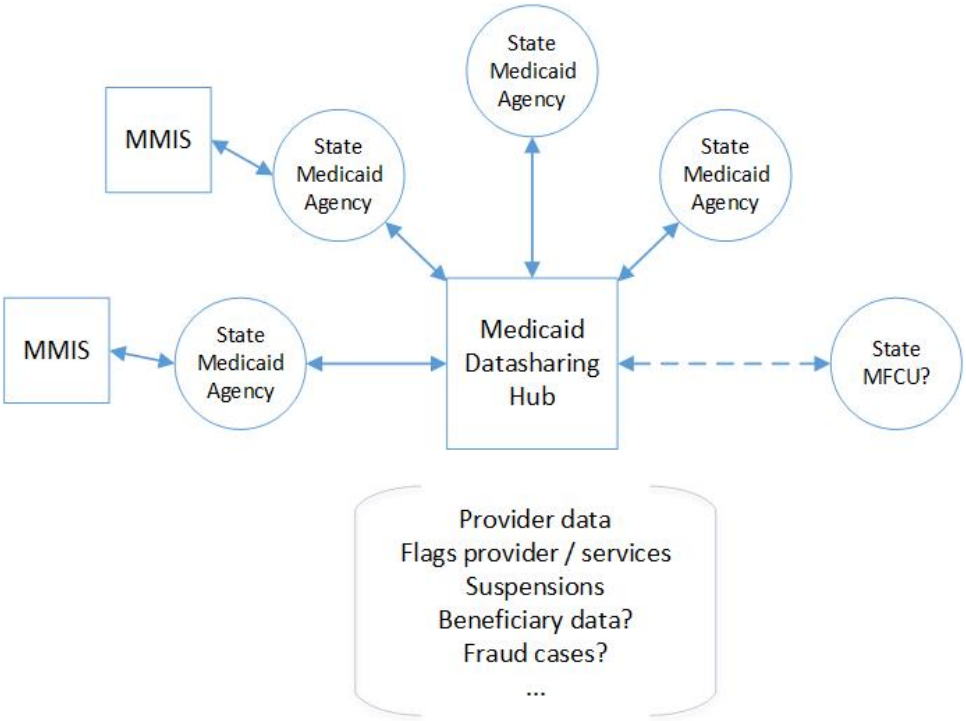

Figure 14 - Federal initiative for national Medicaid data sharing

Organizational view

3. Support Medical Review and Increase Fraud Awareness

We have identified an immediate need to intensify manual claims review, or medical review, during prepayment processing at local state agencies.

Currently only a fraction of the entire claims volume is being reviewed. A 2014 figure for the Medicare program states that just 3 million claims are manually reviewed, from a total volume of 1.2 billion claims yearly (New York Times, 2014).
We were unable to identify reported figures for Medicaid, but the claimed 20% rate in a 2000 OIG report (OIG) sounds almost absurd in comparison. This should further be questioned when considering that some states easily receive more than 50.000 claims each day.
We recall that Medicaid agencies define the first line of defense, and anything that is not detected up to this point, may only be detected after payment is granted. Even worse, a lot of money needs to be spent in postpayment program integrity efforts (either state or federal level) for the identification and recovery of such improper payments.

Increasing Medical Review rate at state level would have two major benefits:

- More fraud referrals originating at early stage, resulting in fraudsters being targeted early and (future) improper claims are to be prevented
- Reduction of money 'wasted' to recover fraud and overpayments throughout the postpayment process

Further benefits of medical review include cost savings to medical plan, the identification of problematic billing practices (those requiring education) and overall increase accuracy in claims processing and payment.

Healthcare leaders should therefore review and take the following actions:

- Increase funding for State Agencies to support increased utilization of Medical Review, split funds from regular PI operations to ensure proper use and allow for monitoring
- Require states to report on manual claim review utilization, introduce metrics to make State Medicaid agencies manual review comparable
- (Require) State agencies to review randomized set of claims, for example adding up to 5% of clean claims (that MMIS approved for payment) per review cycle

The latter is also a means for testing the system and process (on state agency side) for weaknesses, and allows for new insights, or the uncovering of fraud schemes. It partially goes along with gap #1, the lack of utilizing predictive analytics. Staff engaging in Manual Review not only needs to focus on matching medical documentation and ensure medical appropriateness, but also have tools available to manually review the available information; checks which the edits & audits stage did not cover or were able to do.

This in turn drives the need to **increase fraud awareness** at state Medicaid agencies.
Examination of individual claims with supporting documentation does not give the reviewer much information to formulate a fraud suspicion. Review teams therefore need to have broad knowledge, and tools available to investigate on this matter, to be able to formulate a suspicion that can then be investigated further.
CMS should therefore provide additional training for State Agencies specifically targeting their awareness level, technical expertise and to strengthen PI efforts. *As*

this is associated with increased responsibilities for Medical Review teams, their jurisdiction may need to be reassessed.

Likewise CMS should review and update (the) federal regulations as to when providers have to submit additional proof for procedures. Currently defined for certain procedures, CMS should seek to generate additional nationwide thresholds for which manual review is needed.

States Agencies shall need to focus on prevention efforts including:

- Risk-based provider screening,
- Periodic revalidation of enrollment of all providers (<5 years), and
- Temporary suspension of payments while credible allegations of fraud are under further review

For the latter, although legally authorized to do so, and directed by CFR, some states do not suspend payments reasoning missing state authority, missing documentation to support doing so, or the verbal request of the MFCU to in fact NOT suspend payments. Proper authorities must investigate this problem and take actions to align CMS, State Agencies and MFCU, so that payment suspensions can be issued upon first credible allegations of fraud to protect the Medicaid fund.

Another benefit appears that raises fraud awareness at both agency and provider side: An increase of manual claim review, randomization and provider re-evaluation will give providers the feeling that they are in fact reviewed, or their claims are being monitored. The existing scenario shows that providers and claims are barely scrutinized, and those that are not on any watch list (flag) retain a low chance of being targeted in the near future, and less if they do not change their billing patterns significantly to trigger such reviews**.**

The majority of fraud (see fraud types) includes the billing for services that were not rendered (phantom billing), billing for more expensive services, and similar.
Therefore, Medical Review is a very important step in assessing the medical necessity AND legitimacy of providers claims, but should not be limited to the first.
Manual review is the last step before entering the 'pay-and-chase' model, and therefore CMS and State agencies should target (re-)designing Medical Review, along with regulation and necessary jurisdiction.

Possible downsides of increasing medical review could mean more work for MFCUs, as they have to handle a larger volume of fraud referrals, and possibly reduce (chances for) recoveries of overpayments at state or federal PUR initiatives. Alternately, increasing efforts in and funds for prepayment review and fraud prevention would lead to savings in investments that are currently spent on postpayment and recovery initiatives.

Figure 15 shows the improved horizontal fraud control process during prepayment. Highlighted with the added solid boxes, it incorporates our proposals for increased

Medical Review, fraud awareness and fraud referral upon first suspicious, random sampling for manual review, adjustment of flags upon claim suspension and periodic provider re-evaluation.

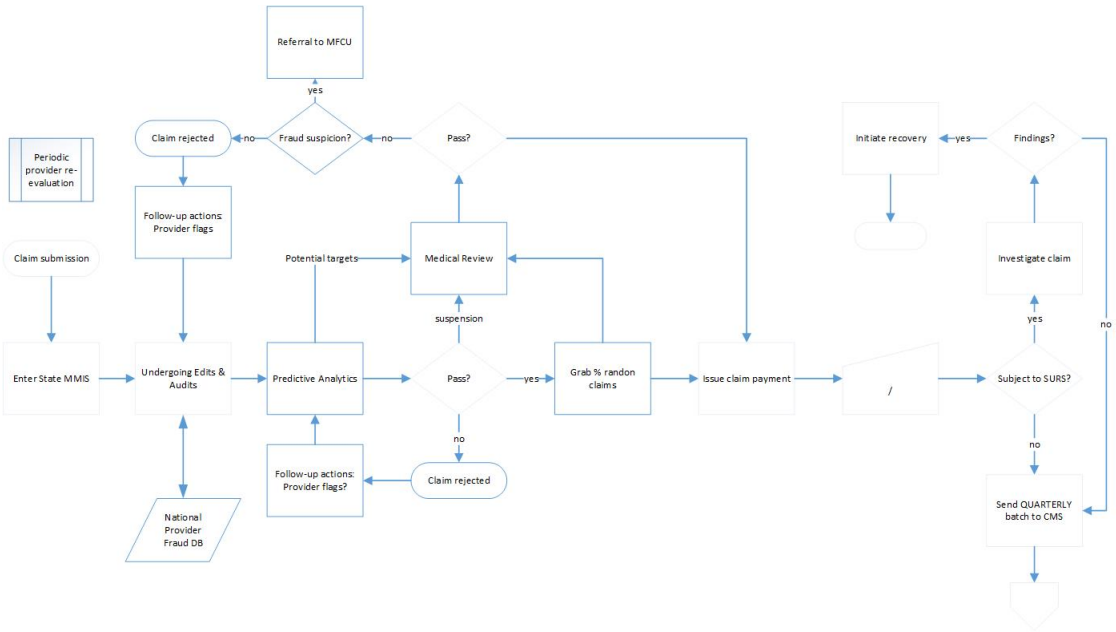

Figure 15 - Proposed fraud control process at prepayment level

6.2 Postpayment safeguards

Process and Technology view

1. Resume federal postpayment auditing

The Medicaid fund is vulnerable. Not only at state level do fraudsters have little trouble to cheat the claims processing safeguards, but also as of mid 2014 they can almost go undetected. Even before this point in time, the federal audit process lacks efficiency. Data is only sparsely loaded into the review system, often with additional months delays because data sets had to be prepped.

CMS must take action and review its entire process pipeline from incoming quarterly batches to feeding of federal utilization review system.
Insights need to be gathered ad hoc to positively influence the development of the upcoming review system, supporting improved process flow, reduced audit cycles and eased collaboration.

In addition, CMS needs to require states to provide well-prepared data sets in a timely manner. With the focus on T-MSIS implementation, CMS needs to collaboratively review and confirm implementation schedules of State Agencies, and if necessary provide help or exert sanctioning for non-compliance.

Upon inception of the new UCM system, preferably with well-advanced progress in state T-MSIS implementation, CMS should streamline and best possibly automate the process chain from receiving quarterly data sets from states, and data loads into the system.

If this process is stable, data extracts and load could potentially be shortened to a 3 months interval. Though this likely has policy implications and might require regulations from outside CMS' control, it would however be beneficial to the fraud control process, and allow for faster overpayments recoveries or fraud detection.

Despite resulting in a noticeable lower than usual ROI (compared to other program integrity initiatives), provider auditing still allow to recovering millions of dollars inappropriately paid. Along with more efficient auditing processes, and the potential of upcoming cross-analysis between Medicare and Medicaid, CMS should increase funding for provider auditing as higher recoveries can be expected.

We note the need to not only focus on auditing the same large provider types (despite the potential of higher recoveries), but also periodically review small providers. It should be in CMS' interest to be on the lookout for and detect real fraudster, or potentially uncover entire fraud schemes, by reviewing a variety of provider types, not be digging in the same holes they have found something before.

Finally, contractors and CMS should reflect on the findings with state agencies for learning, as well as the identification of why fraud or overpayments have or could not have been uncovered earlier.

2. Establish efficient and measurable auditing process

The postpayment auditing process, as shown in Figure 11, is highly sequential, with several steps requiring approval. While the audit itself is tracked centrally, collaboration and communication between the federal agency and contractors occurs via notes or separate telephone calls. Once the assignee changes, several days or weeks go by until the process is resumed.
Recognizing the improved cycle time from before system inception, a 2-year audit cycle is still taking too long – easily taking more if accounting for recovery time and possible appeals.
The entire process of postpayment audit cycle therefore lacks of efficiency, control and measurability.

CMS should re-design the entire process working with contractors, and define time limitations for activities to track the progress and support measuring contractor performance.
This step of improving the process needs to occur prior to the UCM workflow application being completed, as otherwise similar lack of control and inefficiencies can be expected.

It is, however, not just the contractors that CMS has to review and keep track of. The auditing process also shows delayed activities on CMS side.
While it is not known if the re-organization will have an immediate effect, CMS should implement additional oversight on keeping track of the entire auditing process.
Lastly, metrics need to be developed and implemented (and being tracked for) right at the start to maintain control on both internal and contractor performance, as well as corrective action plans must be required to develop if targets are not met.

Separately we note that the utilization of contractors to engage in postpayment auditing complicates the setting, and burdens control on the entre process chain. A radical approach that would benefit from eased collaboration, oversight and likely readily available efficiency would be to discard of auditing contractors altogether, and get specialized people in-house.
Similar to the approach the MFCU is applying (per requirement), by employing teams of subject experts, data analysts and lawyers, teams could specialize on the identification and recovery of overpayment auditing. Such teams would be dedicated towards targeting providers, either by generated target lists as before, or themselves working in close collaboration with the data analytics and control groups, for identifying high-risk areas for potential improver payments and fraud.

Figure 16 shows the how the use of in-house teams could reduce the sequential and approval-dependent process studied in Figure 11 significantly.

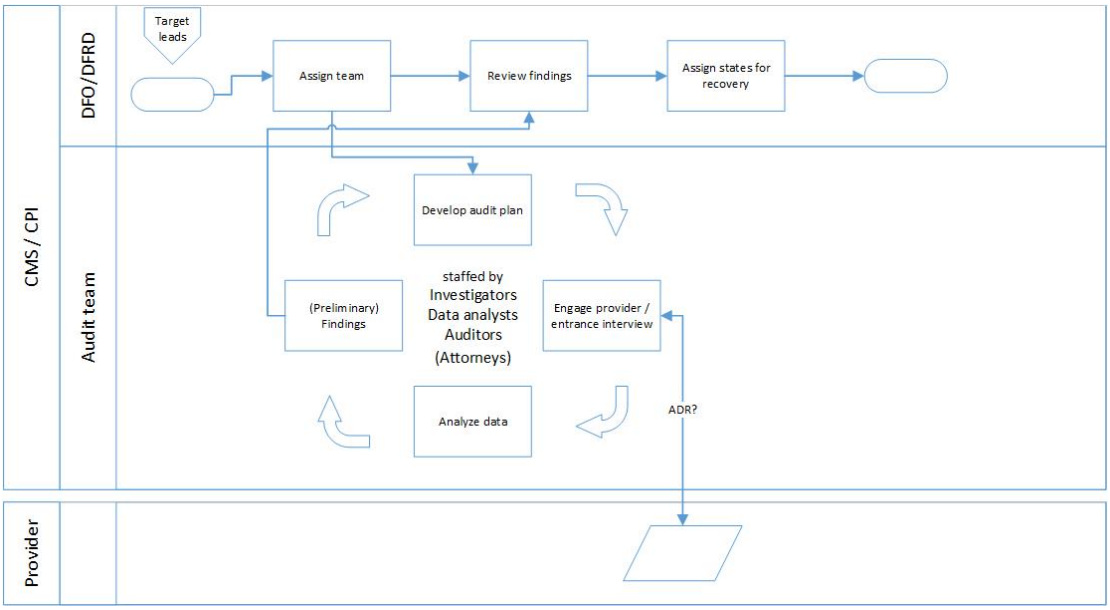

Figure 16 - Iterative in-house auditing

Organizational view (holistic)

3. Implement a coordinated control strategy utilizing a proactive approach

In 2015 the Medicaid fraud control process is still largely based on a pay-and-chase model, with little focus on filtering improper or even fraudulent claims before payment. A centralized, coordinated control strategy appears to be missing, largely owed to the fact that so many entities share responsibilities but also risk control. An entity does just so little as defined by their roles to meet its targets, and stay out of trouble when federal audits review strike.

This is exactly the point where healthcare leaders need to initiate actions.

First, all actors need to become more fraud aware. This is not to say they don't know that fraud is occurring – they do know. But if no party involved has an incentive to find fraud, or is being evaluated against performance of finding 'hidden' fraud, its difficult to engage and commit all entities.

As a result of this, the re-organization at CMS for combining the Medicare and Medicaid program integrity groups has been initiated (other reasons include expanding data transparency across both programs). However, without supplemental steps this approach is not going to improve much itself. It requires continuous monitoring and process improvement, including working with but also evaluating the performance of their contractors. We proposed the usage of contractor metrics in the previous section regarding postpayment audits.

Likewise, we highlighted the need for tighter control for state agencies, as well as their efforts in doing SURS. Currently CMS can only evaluate states for having 'proper' systems and plans in place, but this is not a sufficient enough regulation to enforce states to actually productively and wisely use state of the art systems and actively track down fraudsters and recover overpayments in their programs (which affects the national fund, so it really isn't just a state concern).

While the funds seem to be available for states, it is the states that should be required to gather plans and request funds for updating their PI tools.
Several reports and federal audits have confirmed that State Medicaid SURS subsystems prove to be little effective, highlighted by a June 2014 audit showing one state been cited for lacking its central program integrity function.

This should be reflected by instantiating more fault on PERM rates (and therefore uncovered fraud), so states that use 15+ years old data systems but prove high risk due to their latest PERM assessment must be required to initiate upgrading. Plans should be outlined with the coordination and support of the federal agency.
Most importantly though, CMS must (start to) require states to measure quantifiable benefits, such as cost reductions or avoidance, achieved as a result of operating systems to help prevent or detect improper payments.

Simultaneously, the federal agency inserts additional measures and active controls:
For example federal regulations could authorize CMS to define a per state metrics on sound fraud referrals issued, a minimum rate of yearly recoveries measured against

the most recent PERM rate, or a certain number of payment suspensions due to further investigations each month.

Reversely, the federal agency should coordinate nationwide procedure and provider flags upon first notable reported (a state MFCU handled) fraud case.

Recall gap: Passive role of MFCU / Who actively seeks fraud?
The lack of a single entity having responsibility and jurisdiction to actively look for beneficiary or provider fraud under Medicaid needs to be tackled as well.

Healthcare leaders must establish an "active fraud unit", or otherwise empower the state MFCUs from their re-active mode of handling fraud referrals.
As we have highlighted in the fraud control process, fraud referrals are a rarity, and require enough information to form an actual fraud allegation to support referral.
Increased jurisdiction for MFCUs or the instantiation of a new unit designated for that particular purpose is necessary.
The whole span of control between state agencies and CMS/CPI's postpayment needs to become so fraud-conscious that fraud can be spotted easier and more accurate, but also increase in volume. It would be the responsibility of the receiving unit to request expansion due to understaffing when incoming referrals are stacking up, or otherwise dismiss them due to minor offense.

Federal and state agencies must also ensure that "Medicaid administration personnel have access to the resources they need to combat fraud and abuse." Not only become more fraud-aware, but also provide the necessary tools to and incentives for fraud-referrals, as pointed out earlier. Current tools available lack usability or effectiveness, and federal initiatives are the only solution to this.

Recall gap: Ongoing organizational and technical challenges at CMS
Evaluating the continuous and structural challenges a large federal agency like CMS is facing, only a well-defined strategy including aligning the business and IT environment could solve this dilemma for the long run.
Healthcare leaders need to be brought together from all levels (OIG, CMS, States, MFCUs) to outline a coordinated plan for establishing the setting regarding fraud control matters. While the highlighted re-organizing should largely be finished, structural problems, communication and work agreements between agencies need review.
One radial approach that we like to stress again would be to get rid of contractors – especially regarding federal auditing – altogether and get skilled people in-house, although this remains challenging regarding such a massive healthcare program.

6.3 Review

To cope with the limitations we have identified, we have assessed each of these gaps in more detail, investigating their causes and providing leads that can close these gaps.

We recall once again that states agencies define the first line of defense, and as such they must have all necessary skills and tools available for the mission to stop fraud right from the start (fraudulent claims entering the system domain).

We recommend the following actions:

- Require states to implement 'modern' prevention and data analytics systems (CMS will providing matching funds and technical assistance)
- Require states to measure and report on quantifiable benefits and defined metrics
- Review and enforce stringent PERM rate for State PI units and define clear penalties for deviation, as well as supporting measures and metrics
- Require states to complete T-MSIS transition (withhold matching funds if previous agree-upon schedules not met)
- Continue support state agencies with all means and funds to intensify and strengthen their PI efforts
- CMS to restart and maximize automation for data loads allowing federal postpayment review
- Introduce metrics for contractor's performance (not only audit UPICs), and constrain contracts on meeting targets
- Implement 'active fraud unit' or expand MFCU staffing and jurisdiction

However, the big game changer can only occur with the following - hard to outline and quantify – strategy that would benefit the fraud control program nationwide (opponents are the ones that have a benefit of keeping fraud control inefficient; see corresponding literature review theme):

A coordinated control strategy utilizing redesigned architecture and processes, in other words **architecture-driven fraud control.**

The dispersed structure of Medicaid fraud administration leaves two solution extremes:

- Maintain current state of art while providing state agencies continuous support and funds available, and rely on regulations and existing controls to ensure all units are operating under their target, or
- A federal initiative that includes the design and implementation of an architectural outline specifically designed for this purpose. Unified data models allow for standardization, data transparency; states are required to implement per plan, while increased technical support is offered for the transitioning period

The latter is obviously the favorable; the only problem is to convince healthcare leaders including congress to initiate such a plan. Doing so should severely increase the performance of the overall fraud control process.

7 Validation

This chapter discusses validation and elaborates on the results.

7.1 Validation grounds

Validation is comprised of two parts:
Firstly, open-ended discussion rounds were held with one participant over a period of several weeks into this writing to gather a refined knowledge and insight on processes and the organizational setting involving CMS and its contractors under the domain of Medicaid fraud. In this context discussion was held less formal but with notable contributions:

1) Thoughts and ideas on the issue of healthcare fraud in general have been addressed at an early stage of this writing, and helped steering the analysis and identification of limitations in the proper direction,
2) Potential limitations have been discussed iteratively, to ensure they reflect actual and ongoing flaws that would require action, and
3) Spearheading of initial thoughts on tackling fraud control in a broader context.

Secondary, we used semi-structured, open-ended interview questions with candidates to validate our limitations and results from the previous chapter. Expert opinion was chosen as validation method due to the lack of possibility of actually implementing suggested improvements at state or federal level.
The interviews were semi-structured, meaning that there was room for deviation from the questions stated. The correspondents were also asked to evaluate on the problematic context of healthcare fraud in Medicaid in the larger context.

Two candidates were chosen having a combined previous experience of 10+ years within the fraud control domain in Medicaid, on both academic and practical level.

To safeguard the confidentiality of the participants, the interview questions were formulated in a way that did not require them to reveal sensitive information, further some answers in the remainder of this chapter may have been anonymized.

7.2 Interview questions

The following shows the main questions that were given to the correspondents:

- *How long have you been involved [as contractor] with and exposed to Medicaid, healthcare fraud and control?*
- *What is your perception of the problem of Medicaid or healthcare fraud in general?*
- *What are your experiences in the two key subjects fraud detection and fraud prevention in Medicaid?*

- *What are your opinions regarding the necessity of fraud detection mechanisms, and fraud prevention mechanisms?*
- *Within US Medicaid we talk about prepayment and postpayment safeguards, do you believe one is more important that the other? What is your perception of current target focus by CMS on either?*
- *What do you see as the most critical limitation between state agencies and CMS in its 'joint effort' to combat Medicaid fraud?*
- *What is your opinion towards the lack of a federally shared provider fraud database?*
- *What are your opinions regarding the necessity of state agencies having up-to-date access to national and federal data marts for prepayment claim validation?*
- *What are your opinions regarding the necessity of either a federally hosted and shared fraud tracking system, or a hub and spoke architecture interfacing with the MMIS systems of state agencies? Would you favor one over the other?*
- *A hub and spoke architecture could provide future opportunities for states to exchange various kind of information ad hoc for pre screening, but a nationwide initiative would be costly and time-consuming. What are your thoughts?*
- *What is your opinion on progress of predictive analytics implemented at state or federal level under Medicaid?*
- *Where do you think predictive analytics should be focused, and whose responsibility it should be?*
- *If claims pass all edits and audits they will rarely be subject to Medical Review. What options and opportunities do you see at this point?*
- *From your experience, do you think that collaboration between State Agencies and state MFCUs is working well, is efficient?*
- *What is your perception of the progress in combating Medicaid fraud on national and federal level over the past few years?*
- *In general, what key organizational changes do you think are needed to improve fraud detection and prevention efforts? (National or Federal)*
- *In general, what key technical changes do you think are needed to improve fraud detection and prevention? (National or Federal)*

In chapter 7.3 we summarize our findings from interviewing our two subject matter experts, and their broader view on the issue of fraud control in US Medicaid.

7.3 Validation results

7.3.1 Interview #1

The first interview was conducted with a person previously working as contractor to CMS at the MIG DE project, with additional domain experience as practitioner and researcher in data analytics for 3+ years.

In characterizing the problem of Medicaid fraud, the participant first described Medicaid as facing an organizational problem where responsibilities are unclear when it comes to combating fraud. In fact, nobody seems to be 'in charge' when looking for strategic elements of nationwide control. Rather it's a somehow 'political game' where people involved contribute as much as to meet their targets, but not more.
The participant also noted the difference of program implementations between countries. Where in other healthcare program settings claims are verified before, under Medicaid there is a high percentage automated and payment granted for the majority of billed services without doing so. The fact that doctors in the US have a high status (occupational prestige) may be related.
When it comes to program integrity efforts, the participant notes that it doesn't seem to be a budgeting problem. Program integrity costs millions of dollars yearly, but due to the majority of efforts resulting in positive ROI this is sound.

The participant favors prevention over detection of fraud. While a solid prevention effort should only be 'designed once, detection is something that will always happen'. It's reoccurring, because detection techniques always need to be modified, expanded and reviewed.
However in any likable situation one will end up with both, but prevention can save more. Medicaid current focus is more on fraud detection over prevention.

In comparing the payment processing efforts to other countries, it was noted that the Netherlands for example have a way 'higher rate in Medical Review', also due to higher regulations of when supporting documentation has to be sent in and manually verified. Combinations of rules in the edits and audits stage was also reported to be very limited with a higher potential for verification left open.

The participant characterized the 'need for states to have (a high) responsibility for finding fraud'. Although states and the federal level share costs for claims under Medicaid, there is a somewhat lack of responsibility for finding fraud at either sides. If no fraud is found the costs for both may rise, but without a way of measuring such, and shares will remain nevertheless. The participant recommends a ways for cost control to break this interdependency and incentivize states for finding fraud.

A (national) fraud database should be in place our participant strongly recommends. While different implementations at state levels exists, there should not be any technical limitation that such national fraud database could not be established, and states required to submit to, and use information from that database. Such provider

database must be operated and maintained by the federal agency, and is needed funds be made available for states to integrate with this solution.

Regarding state agencies having up-to-date access the respondent highlighted that the concern would be more of the data quality and usability states have when accessing or comparing such information.

A federal initiative for a hub-and-spoke architecture to integrate states MMIS is considered possible, but concerns were raised on the organizational aspect rather than technical aspects. Who's in charge for such implementation, who guarantees participation, who will pay for it and who is going to be incentivized?

The participant described that there barely is (if any) fraud prevention in Medicaid at federal level; however, some states have started implementing predicative analytics. Again the need for clear incentives for states are needed to get all 50 states committed for increased fraud prevention efforts.

Additional concerns were raised when talking about claims processing and manual review. The chance of a provider being reviewed is very low in the current situation, as we have outlined earlier. Our participant explicitly states that 'enough review should be done to give providers the feeling that they are (indeed) being checked'. By expanding the usage of and lowering current thresholds, more procedure need to be 'flagged for medical review' prior to payment.

Concluding our participant noted that the problem [of healthcare fraud, Medicaid fraud] is not as huge as Sparrow has described it in his 2000 assessment. That is, over the past years there has been progress, however, other countries are far more advanced in combating fraud within their programs. While Medicaid is yet so different compared to centralized programs, it continues to need special consideration and continued efforts in program integrity. The expected increase of enrollees and therefore rising costs due this program 'won't be the problem'.

Review of limitations:

(Prepayment)

1. Lack of predictive analytics or similar prevention mechanisms in place

Severity: High

> 'It is not the predictive analytics (predicting the future of claim amounts) but the current insight to fraud experts what 'profiles' providers have in their submission pattern. Knowing the cost of a provider, what he is claiming on average, is that normal compared to similar peers? […] This information is lacking and could make huge improvements in the time to detect a fraudulent activity, which now with the overpayment analysis is almost 2 years.
>
> Second, also quite high are the prevention mechanisms but more on the regulatory side of CMS […] about what providers may submit, before they have to add additional proof to their need of larger quantities of claims.'

2. Lack of Validation against other State's Beneficiary/Provider flags or federal databases

Severity: Medium

> ‘Not per se high. A lot can be done by using thresholds and rule based systems as well, I believe that visualizing a providers profile is more important than comparing it to other providers. Fraud experts can't review individual claims, but do know if 100 claims of type E678Y is normal for provider X under Medicaid Kansas.
>
> It is really important to check whether the provider has frauded in different states [before], […] it is a nation wide program, so there should be information services sharing this kind of knowledge, or registered federally.’

3. Low Utilization of States’ Medical Review / Fraud Awareness

Severity: Medium

> ‘They are aware of the fraud, but you'll end up negotiating the prices including the fraud, rather than fighting the fraud [as such]. This is usually because they know both what was done was wrong, but it is hard to proof who did wrong. Doctors just claim in the wrong way (or their assistants). Only in certain cases of obvious fraud they may directly suspend payments and prosecute.’

(Postpayment)

1. Delayed / Halt of data loads for CMS postpayment review

Severity: High

> ‘Goes along with prepayment limitation #1 [prevention efforts]. If postpayment data load is monthly, than it is quick enough to spot hit and run fraud. Business Intelligence at prepayment “foresees” in the same information need aspect.’

2. Postpayment auditing inefficiency

Severity: Low

> [In a response to ‘Federal audits digging in the same holes’]: If they search in the same holes, why not prevent them in the first place. Somehow, people still try [to overcharge or fraud]. Efficiency does not make to much sense here; it only affects the money flow for CMS that comes in a little later.

3. Passive role of MFCU / Who actively seeks fraud?

Severity: Medium-High

> ‘Who is responsible, has targets to meet and is reviewed for its performance? Is MFCU? Fraud is in the financial sector a ROI and managed risk game. Under Medicaid, not sure if they approach it this way.’

4. Ongoing organizational and technical challenges at CMS

Severity: Low-Medium

> ‘It is better for them [CMS] to not contract, but get the people in house. But those are the same mistakes as the Dutch government makes as well.’

7.3.2 Interview #2

The second interview was conducted with a longtime practitioner and researcher in Medicaid fraud, with domain experience including system design and architecture as contractor to CMS for several years.

The participant initially characterized the problem of Medicaid as 'bad because there doesn't seem to be a true desire to address it' really. 'No independent party is charged to check what is really going on', except for sparse OIG audits reviewing the program from time to time. Moreover, 'not much money is spent on combating fraud' under Medicaid and Medicare either [in relation to the scope of the problem].

Although the 'MIG was originally supposed to actively look for fraudsters' in the program, as of now there is not unit tasked with actively targeting potential fraudsters prior to MFCU's working on formulating cases when reasonable allegations of fraud have been found 'by chance'. Our participant therefore defines the need to 'create a unit that actively looks for fraud'.

Another concern raised was the political power that provider's have or may exert when they do not receive money for claim reimbursements in a timely manner (or to their desire). It appears that such power is 'virtually' superior to state agency regulation of paying within their 90 days windows.

From another viewpoint our participant clarified that 'reimbursement rates [under Medicaid] are low, and if it get more difficult to bill, it doesn't pay physicians enough so potentially they are de-rolling'. Therefore, more safeguards make their life more difficult. This poses a risk for CMS and states that these [healthcare programs], safety nets targeted for poor people, will be discarded by honest providers.
There are indeed 'challenges to check for legitimacy of claims', and 'not many ways to differentiate fraud from improper billing' for either state or federal side.

The participant stated that "**states have no incentive to find fraud**. They're just paying".

Especially regarding fraud prevention not much focus is spent on controls. For example, once medical providers are enrolled in the program, they can 'bill whatever they want'. Some pre-screening is done, but only targeting whether the providers hold legit licenses and have no criminal background or alike. A federal initiative of having contracted out the evaluation and scoring of providers prior to enrollment does not overcome this issue.

Regarding the necessity of fraud detection and prevention mechanisms our participant positions that 'no long term analysis on (overpayment)charges [are] reasonable. Some kind of rational is needed to kick people out [of the program upon first allegations of fraudulent actions].' As we have shown, the federal focus is on targeting overpayments and recovering money, sometimes years in the past. This should not define the main focus of the federal agency for the next years.

Likewise the important of prepayment review was stressed. ‘The more prepayment, the less to chase’. By ‘using knowledge, systems and models that have been uncovered or defined under postpayment’ should be used in prepayment stages. For example the definition of an algorithm targeting overpayments for specific dental services that proved to be abused frequently should be carried over so that states can use the same analysis to prevent such abuse in the first place!

The biggest issue [critical limitation between state agencies and CMS| is the alignment. Again, no one has an incentive for finding fraud, and an agency need to be granted sufficient power to not only oversee but also actively administer fraud control. The OIG could potential be tasked with such a role.

While the ‘technical challenges of e.g. national warehouse could be overcome, the political initiative needs to happen’ first.

Our participant stressed the **lack of fiscal checks** during payment validation. There is ‘not enough traceability of where is the money going, whether it really is the practice of a doctor or an offshore account’. This problem is increased by the fact that third parties are charged with billing for doctors. Audits are needed to identify characteristics of billing agencies, to identify and stop potential billing fraud and abuse.

Concluding our participant highlighted the **political challenge** of Medicaid fraud. Technical challenges can be overcome, but it is the lack of incentives for finding fraud and the **lack of an empowered entity** that to administer a coordinated fraud control program. One suggestion would be to empower the OIG to do so, and task CMS to enable set plan, but stringent requirements and controls are needed so that commitment is ensured and progress can be tracked.

8 Discussion

Interview results
The interviews were conducted to obtain additional insights into the field of Medicaid fraud, from knowledge and experience of long-time practitioners. The interviews indeed provided additional thoughts on the context, but also confirmed the 'hot topics' from both identified limitations and recommendations for actions. Both participants stressed the urgent need for a top-level initiative to address the issue of fraud in Medicaid. While concerns were raised regarding additional controls that could make claims submissions harder for the honest providers, both practitioners agreed that states must engage in more prepayment activities. While technical challenges can be overcome, and not many concerns were raised regarding available funds; the most critical aspect is outlined by the lack of incentive for state to find fraud. Our interviews further confirmed that little focus is spent on preventing fraud in the first place, and doing so can significantly decrease efforts spent on postpayment review and recoveries of overpayments.

Additional findings
An interesting observation has been made regarding the regulative side: The **False Claims Act** (see section 1.1.7), a major tool for identifying fraud that incentivized individuals to report such, is not enacted in all US states but 30. While the reasons and impact are outside the scope of this research, other states benefit from millions in recoveries due to this law.
Fraud in healthcare is a form of **white-collar crime**, which makes it hard to tackle. White-collar crime exists (to some extend) in every society, causes are manifold and include individuals not having the same frame of reference when it comes to what is wrong and what is right, or factor contributing to the temptation of individuals due to lack of imposed sanctions, or the suffering from financial challenges. Healthcare fraud described a moral dilemma, and fighting white-collar crime must be initiated on several levels, including awareness and training to people involved, communication of the effects, but also by setting examples.

Reflection
Current mitigation efforts in Medicaid found to be ineffective and inefficient. Barely any fraud control exists, as states administer their program and PI initiatives and the federal agency has little control over states. Federal agency is left with searching for improper payment on years old data. Fraud prevention efforts are almost entirely missing at state level. The fact that CMS has stopped data loads in prospect of an UPCOMING central audit-tracking platform also does not allow for overpayment recoveries during postpayment review since last 2014.

Literature and our review revealed that despite awareness of and attention paid to healthcare fraud, combating fraud in both Medicare and Medicaid programs remain a challenge. As part of the revised and expanded Medicaid eligibility due to the Affordable Care Act (ACA) from 2010, Medicaid program costs will increase.
Unlike Medicare, Medicaid is not centrally administered, and its structural features make nationwide program integrity efforts challenging.

We have identified a number of critical limitations in the current fraud control process, which span over organizational, process and technological aspects. The need to address these limitations is crucial if the Medicaid fund is to be protected from wasting hundreds of millions of dollars due to fraud, waste and abuse.

Healthcare leaders including CMS, State Agencies and governing bodies under current regulations can do a much better job in fighting fraud. But this requires joint effort of all parties and a coordinated fraud control strategy.

9 Conclusion

This chapter presents the conclusions of this research. The research questions outlined in 1.2.4 are answered, followed by a description of the contributions for literature and practice in section 9.2. Sections 9.3 and 9.4 conclude this chapter by discussing the limitations of this research and opportunities for future work.

9.1 Conclusions

To answer our main research question, we first provide answers to the five sub-questions:

1. *What is the current state of Fraud Detection and Prevention in Medicaid?*

This research question has been answered two-fold; with an initial literature review, and a detailed analysis of currently deployed safeguards and processes:

Literature revealed a continued lack of evidence about the magnitude of healthcare fraud. Due to the invisible nature of this problem, no measures exist and reported estimates differ to a great extent. Means of electronic fraud detection remain poorly researched and people charged with finding fraud may not be able to grasp upon the full potential of utilizing toolsets that may be found suitable. We also identified missing research into current state descriptive study, especially research on processes or relationships that involve agencies like CMS and State Medicaid Agencies.

While literature presents awareness that healthcare fraud diverges over many disciplines, not all themes have been researched to a proper extent.

Our further study revealed that current practices in Medicaid focus on detection over prevention, and both efforts perform rather poor considering the magnitude and impact of the problem in the larger context.

2. *What are existing safeguards controlling Medicaid?*

A literature and document review was conducted to identify currently deployed mechanisms for controlling Medicaid fraud. It has been found that such mechanisms can be split between two extremes, the prepayment and postpayment safeguards.

We have identified 4 major control systems, each in turn comprising of a variety of sub-systems or safeguards. The four control systems are described as:

- Claim Processing and Edits and Audits
- Prepayment Medical Review (Manual Claim Review)
- Postpayment Utilization Review (SURS, PUR)
- Special Investigative Units (MFCU)

In Medicaid, a number of actors are involved at separate stages, and contribute or control parts of these safeguards. The fraud control process further differentiates between the different stages involved.

3. *What intra- and inter-organizational processes are currently deployed to support these safeguards?*

To answer this research question we utilized document reviews and domain experience to model processes representing the prepayment and postpayment phases. For the latter, we additionally took advantage of process mining to analyse the federal postpayment utilization review (PUR) process from system insights. We describe the entire process chain from claim inception to possible fraud referral onto law enforcement the **fraud control process**. This control process includes a variety of sub-processes separated or shared between participating actors charged with control activities. Actors are representing state and federal level; three separate units are directly tasked with fraud control, and a number of contractors are used to support or 'outsource' a number of activities.

Processes have been identified and modeled at state level involving claim inception, edits and audits check, manual claim review, disposition for payment, SURS and sending of quarterly data sets to CMS. CMS receives postpayment data from states, stores and converts data, and loads data into designated systems to support federal postpayment review and data analysis purposes. The audit process targeting a provider to identification and request of overpayments is also modeled.

4. *What are gaps in deployed safeguards that mitigate fraud control in Medicaid?*

From this review we were able to identify and pinpoint a set of limitations, which were coded into a set of broader themes – each of which revealed additional issues outlined under chapter 5. Table 3 lists these themed gaps that have been identified per 2015 assessment of Medicaid fraud control processes and safeguards implementation. The severity assessment is adjusted based on insight from the first interview.

Table 3 - Themed limitations

Prepayment		Adj. Severity
	Lack of predictive analytics or similar prevention mechanisms in place	High
	Lack of Validation against other State's Beneficiary/Provider flags	Medium - High
	Low Utilization of States' Medical Review / Fraud Awareness	Medium
Postpayment		
	Delayed / Halt of data loads for CMS postpayment review	High
	Postpayment auditing inefficiency utilizing DE	Low - Medium
	Passive role of MFCU / Who actively seeks fraud?	Medium - High
	Ongoing organizational and technical challenges at CMS	Medium

The two most critical limitations are the lack of sufficient prevention mechanisms, including predictive analytics at the prepayment stage, as well as the currently halted data load of Medicaid claims data into federal review system to allow CMS and contractors the identification of fraud and overpayments on recent claims.

5. *How can current processes and safeguards be improved to strengthen Fraud Detection and Prevention in Medicaid?*

From our analysis of current Medicaid fraud control processes and safeguards, the following need and recommendations for improvement emerged:

- Require State Agencies to implement 'modern' prevention and predictive analytics systems
- Implement ways for cross-state validation of Beneficiary/Provider flags; a federal initiated (fraud) data sharing system is critical!
- Require states to measure and report on quantifiable benefits and defined metrics
- Review and enforce stringent PERM rate for State PI units and define clear penalties for deviation, as well as supporting measures and metrics
- Require states to complete T-MSIS transition (withhold matching funds if previous agreed-upon schedules not met)
- Continue to support state agencies with all means and funds to intensify and strengthen their PI efforts
- CMS to resume and maximize automation for data loads allowing federal postpayment review until UCM takes over
- Introduce metrics for contractor's performance (not only audit UPICs), and constrain contracts on meeting targets
- Implement and authorize 'active fraud unit', or expand current MFCU staffing and jurisdiction

Our validation with expert opinion confirmed the critical need for increased prevention mechanisms, a federal led data sharing initiative and an empowered entity that is tasked with actively finding fraud.

How can intra- and inter-organizational processes and safeguards for Fraud Detection and Prevention in US Medicaid be improved?

In addition to our previous recommendation, we identified – and our interviews confirmed – the urgent need for federally led initiatives that not only include the implementation of missing tools to support states, but a central coordinated fraud control strategy.
All stakeholders involved seem to be doing the very minimum of what they are asked to do. The problem that no stakeholder (tasked with fraud control) has clear incentives for finding fraud must be addressed immediately.
The need for an empowered entity with oversight and control mechanisms over CMS and State Agencies is imminent. One participant suggested that CMS may lead the progress on implementation and continue supporting the states, but overall administrative (!) oversight and independent evaluation of progress must be done by another unit, e.g. OIG.

9.2 Contribution

This section indicates how this research contributes to Medicaid fraud (control) practice and theory.

Contribution to literature
From our literature review we identified the lack of research into current state descriptive study, especially focusing on Medicaid fraud control. Further we could not find literature that provided analysis on the processes and responsibilities between agencies involved in combating fraud in US healthcare. Where previous literature focused on applying single methods for data analysis, improving the eligibility process, constructing unified data models and alike, this research provides a holistic view on intra- and inter-organizational processes, presenting the most relevant actors participating in fraud control in US Medicaid.

By studying literature, system and audit documents, a contextual overview of the current state of Medicaid fraud detection and prevention efforts was presented, and the fraud control process was visualized. The setup of explicit models allowed us to analyze in depth the current situation, and to identify limitations that were previously disguised under the complexity of the domain or overstatements by healthcare leaders. The proposing solution strategies and validation expands literature further, while providing a road map where future research should focus on.

Contribution to practice
The identification and presentation of gaps shows lacks of program integrity efforts. By presenting a thorough analysis on processes involved in, and limitations to fraud control efforts, a holistic overview as presented might aid healthcare leaders such as CMS and OIG, and lawmakers to re-assess current PI efforts and regulations.

The paper urges awareness for staff members tasked with combating fraud, waste and abuse as part of their daily work. Despite working within their prescribed roles, it is the commitment and extra eager that is required to strengthen fraud control on a larger scale.

Reading of this paper can also serve as reminder for beneficiaries to be on lookout, and raise voice if faced with alleged fraud. Public awareness and understanding of Medicaid billing and fraudulent behavior might raise concerns of beneficiaries who become more inclined to ask or provide leads of suspicions.
The public awareness by study publication, and continued research into subject domain are further contributions this paper provides.
Finally, healthcare leaders can read chapter 5 and 6 as recommendations for practice, a thorough re-assessment has the potential to mitigate lack of fraud control in the long run.

9.3 Limitations

The following limitations of this research can be derived:

One limitation is the scope of this paper versus the scope of the problem of healthcare fraud. We determined earlier that researchers have acknowledged that the issue of healthcare fraud is not subject to one discipline (Sparrow, 2000, Lorenz, 2013), but must be tackled on several levels. We provided a holistic overview on business, process and technical level, but this does not cover the full understanding of ties and problems in this domain.

Another limitation is represented by the source of information that contributes to development of this thesis. Documents and reports from the state and federal agencies might be biased, and reported figures be extrapolated to meet agency targets or satisfy the public. The first scientific author used open coding on reviewed documents and accumulated domain knowledge in order to conceptualize the AS-IS situation. This action is unbiased as the author is not a beneficiary of US healthcare, not a participating member of fraud detection practices and has no financial stake in this review. Process models were not solely established from literature and document reviews, but supported by domain insight, discussion with subject matter experts and actual work system review using process mining.

Because of the complex issue and distributed nature of Medicaid fraud control, recommendations suffer from practical approaches. While we point to several aspects that have been identified as major flaws in current efforts, recommendations target a variety of stakeholders and the need for a coordinated control strategy is not readily applicable. Our two interviews with experts however confirmed most of our analysis and recommendations, and it is up to the people in charge to initiate action.

9.4 Future Work

This thesis provides a number of interesting opportunities for future research and practices.
Firstly, more research is required in the subject of Medicaid fraud, particularly regarding technical possibilities for fraud prevention. Even though the Medicaid program poses structural challenges, improving fraud prevention comes at the benefit over having to recover or identify fraud at a later stage. More possibilities should therefore be explored, and whether existing controls from other programs can be transferred to the Medicaid program.

Qualitative research could explore limitations in Medicaid fraud control efforts by interviewing or surveying state agencies and staff, obtaining their view on regulations, constraints or opportunities like assistance and funding to support their control efforts. While funding for initiatives might be available, it is possible that state agencies cannot readily access those funds due to regulations, contracting issues or are otherwise reluctant to initiate such process.

More exploratory research should be done to uncover the state of implementations and usage for fraud detection and prevention mechanisms at state agencies and PI units, and the skills of personnel working with such.
Since state administer their PI efforts themselves and CMS only provides technical assistance, studies need to explore if the right people are tasked with the right (and suited) responsibilities, or whether states just comply to the minimum set of guidelines (as we have indicated).

We would also like to see research into the perception of fraud control **progress** using a broader target group. A qualitative approach using surveys could identify the perception of program integrity progress for a variety of stakeholders; beneficiaries, state agencies, federal agencies, providers and billing parties. Increase of fraud control efforts may also be seen as a downside for the providers and billing agencies running legitimate businesses, but having to face more hurdles and possibly withdraw from Medicaid programs.

Another recommendation for further study includes research into policy implications. That is, what policies are needed to be addressed at state and federal level to increase incentives for people to find fraud. This issue has been stated prior and confirmed by our interviewees. Research should further pinpoint to what are applicable methods, tools or regulations balancing an allowed but also enforced state of finding fraud.

As for practice recommendations, it is the willingness to engage all stakeholders participating in fraud control to exert their commitment in a larger context, and healthcare leaders need to re-assess their own strategies; CMS must review it's Medicaid Integrity Plan, seek and implement process improvements throughout its integrity program, support organizational change as needed, and increase or re-design technology usage that is lacking or proving insufficient.

References

42 U.S. Code (2015) - *Fraud and abuse control program*, http://www.law.cornell.edu/uscode/text/42/1320a-7c, retrieved on December 3, 2015

42 CFR (2015) - Public Health, https://www.law.cornell.edu/cfr/text/42, retrieved on December 3, 2015

Bai X. et al. (2012), A decision methodology for managing operational efficiency and information disclosure risk in healthcare processes, 10.1016/j.dss.2012.10.046

Agrawal et al. (2013), *Expanding Physician Education in Health Care Fraud and Program Integrity*

Chen, S. & Gangopadhyay A. (2013), *A Novel Approach to Uncover Health Care Frauds Through Spectral Analysis*, DOI 10.1109/ICHI.2013.77

CMS (2014), *Comprehensive Medicaid Integrity Plan - Fiscal Years 2014 – 2018*

CMS (2014), CPI, *Annual Summary Report of Comprehensive Program Integrity Reviews - June 2014*

CMS (2011), *CPI Key Antifraud Activities*

CMS (2014), FPS - *Report to Congress Fraud Prevention System Second Implementation Year - June 2014*

CMS, Medicaid Integrity Program - General Information**,** http://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/MedicaidIntegrityProgram/index.html, retrieved on December 6, 2015

CMS, Medicaid Integrity Program Manual, 100-15

CMS, Medicare Program Integrity Manual, 100-08

Copeland L, et al. (2012), *Applying Business Intelligence Concepts to Medicaid Claim Fraud Detection*. Journal of Information Systems Applied Research

Ekin T et al. (2013), *Applications of bayesian methods in detection of healthcare fraud*, DOI: 10.3303/CET1333026

GAO, (2014), *MEDICARE FRAUD - Further Actions Needed to Address Fraud, Waste, and Abuse*

HHS (2015), *National Medicare fraud takedown results in charges against 243 individuals for approximately $712 million in false billing*, http://www.hhs.gov/about/news/2015/06/18/National-Medicare-fraud-takedown-results-in-charges-against-243-individuals-for-approximately-712-million-in-false-billing.html, retrieved on December 6, 2015

The Huffington Post (2014), *U.S. Experiences Unprecedented Slowdown In Health Care Spending*, http://www.huffingtonpost.com/2014/12/03/health-care-spending_n_6256166.html, retrieved December 1, 2015

Joudaki et al (2015), *Using Data Mining to Detect Health Care Fraud and Abuse: A Review of Literature*, 10.5539/gjhs.v7n1p194

Kaiser Family Foundation (2015), Total Medicaid Managed Care Enrollment, http://kff.org/medicaid/state-indicator/total-medicaid-mc-enrollment, retrieved on November 28, 2015

Kaiser Family Foundation (2015), Total Monthly Medicaid and CHIP Enrollment, http://kff.org/health-reform/state-indicator/total-monthly-medicaid-and-chip-enrollment/, retrieved on November 28, 2015

KHPA (2010), OIG, *A Performance Audit of Kansas' Medicaid Claims Processing*, Kansas

Kirschner N. et al (2014), *Prescription Drug Abuse: Executive Summary of a Policy Position Paper From the American College of Physicians*, doi:10.7326/M13-2209

Laursen, K. K. (2014), *Leadership Strategies and Initiatives for Combating Medicaid Fraud and Abuse*

Lewis Morris (2009), *Combating Fraud In Health Care: An Essential Component Of Any Cost Containment Strategy*

Li J. et al. (2007), *A survey on statistical methods for health care fraud detection*, DOI 10.1007/s10729-007-9045-4

LII – Legal Information Institute (2015), Healthcare Fraud, https://www.law.cornell.edu/wex/healthcare_fraud, retrieved on December 10, 2015

Liu, Q., & Vasarhelyi, M (2013). *Healthcare fraud detection: A survey and a clustering model incorporating Geo-location information*. In 29th world continuous auditing and reporting symposium (29WCARS). Brisbane, Australia

Lorenz, F. A. (2013), *Healthcare Fraud in the United States: Assessing Current Policy and its role in Fraud Prevention*

McKnight's (2015), *CMS plans fraud-tracking system*, http://www.mcknights.com/news/cms-plans-fraud-tracking-system/article/417265/, retrieved on December 6, 2015

Morris L. (2009), *Combating Fraud In Health Care: An Essential Component Of Any Cost Containment Strategy* in HealthAffairs, 28, no.5 (2009): 1351-1356, doi: 10.1377/hlthaff.28.5.1351

National Association of Medicaid Fraud Control Units (NAMFCU) (2015), About MFCU, http://www.namfcu.net/about-us/about-mfcu, retrieved on December 6, 2015

New York Times (2014), *Pervasive Medicare Fraud Proves Hard to Stop,* http://www.nytimes.com/2014/08/16/business/uncovering-health-care-fraud-proves-elusive.html, retrieved on December 6, 2015

Ngufor, C., & Wojtusiak, J. (2013), *Unsupervised labeling of data for supervised learning and its application to medical claims prediction*

Office of the Legislative Counsel (2010), *Compilation of Patient Protection and Affordable Care Act (ACA)*, http://housedocs.house.gov/energycommerce/ppacacon.pdf, retrieved on December 6, 2015

Ohio MITS – Claims, Edits, Audits, EOB Participant Guide, 2010

OIG (2014), CMS System for Sharing Information About Terminated Providers Needs Improvement, OEI-06-12-00031,

OIG (2000), Medicaid Proactive Safeguards, OEI-05-99-00070

OIG (2000), Medicaid Claims Processing Safeguards, OEI-05-99-00071

OIG (2000), Medicaid Post Payment Safeguards, OEI-05-99-00072

OIG (2014), MFCU STATISTICAL DATA FOR FISCAL YEAR 2014

OIG (2015), Semiannual Report to Congress

Olsen P. et al (2014), *Graphical Models for Identifying Fraud and Waste in Healthcare Claims*, DOI: 10.1137/1.9781611973440.66

Ortega P. A. et al (2006), *A Medical Claim Fraud/Abuse Detection System based on Data Mining: A Case Study in Chile*

Phillips, J. (2012), *Prescription drug abuse: Problem, policies, and implications*, DOI 10.1016/j.outlook.2012.06.009

PR Newswire (2009), *Waste in the U.S. Healthcare System Pegged at $700 Billion in Report From Thomson Reuters*, http://www.prnewswire.com/news-releases/waste-in-the-us-healthcare-system-pegged-at-700-billion-in-report-from-thomson-reuters-65969017.html, retrieved on December 6, 2015

Saldana, J. (2012), *The Coding Manual for Qualitative Researchers*

Schaum K. D. (2015), *Don't Let Your Revenue Be Part of the $4.9 Billion Returned to Taxpayers!*

Sparrow, M. (2008), Fraud in the U.S. Health- Care System: Exposing the Vulnerabilities of Automated Payments Systems

Sparrow, M. (2000), *License to Steal*

Srinivasan U. and Arunasalam A. (2013), *Leveraging Big Data Analytics to Reduce Healthcare Costs*

Strauss, A.L., Corbin, J.M. (1991), *Basics of qualitative research grounded theory procedures and techniques*, vol. 6. Sage, Newbury Park

Suleiman M et al (2014), *Data Driven Implementation to filter fraudulent medicaid applications*

Thornton et al (2013), *Predicting Healthcare Fraud in Medicaid: A Multidimensional Data Model and Analysis Techniques for Fraud Detection*

Thornton D. et al (2014), *Outlier-based Health Insurance Fraud Detection for U.S. Medicaid Data*

Thornton D. et al (2013), *Predicting Healthcare Fraud in Medicaid: A Multidimensional Data Model and Analysis Techniques for Fraud Detection*

Travaille et al (2011), *Electronic Fraud Detection in the U.S. Medicaid Healthcare Program*

TruvenHealth (2014), Medicaid Program Integrity: *Fighting Fraud in a Managed Care Environment*, http://truvenhealth.com/blog/medicaid-program-integrity-fighting-fraud-managed-care-environment-16, retrieved on December 6, 2015

van der Aalst (2011), *Intra- and Inter-Organizational Process Mining: Discovering Processes within and between Organizations*

Van der Aalst, W.M.P. 2011. Process Mining: Overview and Opportunities. ACM Trans. Manag. Inform. Syst. 99, 99, Article 99 (February 2012), 16 pages. DOI = 10.1145/0000000.0000000

Weng X., Shen J. (2008), *Detecting outlier samples in multivariate time series dataset*, doi:10.1016/j.knosys.2008.03.048

Weijters, van der Aalst, Alves de Medeiros (2006), *Process Mining with the Heuristics Miner-algorithm*

WSJ (2008), Medicare, *Medicaid Managed Care Gets Scrutiny for Fraud*,
http://www.wsj.com/articles/SB120589320981247561, retrieved on December 5, 2015

Wulf V. & Rohde M. (1995), *Integrated Organization and Technology Development – an Approach to Manage Change*

Wulf V. & Rohde M. (1995), *Towards an Integrated Organization and Technology Development*