United States Government Accountability Office

Report to Congressional Requesters

August 2017

MEDICARE

CMS Fraud Prevention System Uses Claims Analysis to Address Fraud

Accessible Version

GAO-17-710

August 2017

GAO Highlights

Highlights of GAO-17-710, a report to congressional requesters

MEDICARE

CMS Fraud Prevention System Uses Claims Analysis to Address Fraud

Why GAO Did This Study

CMS analyzes Medicare fee-for-service claims data to further its program integrity activities. In 2011, CMS implemented a data analytic system called FPS to develop leads for fraud investigations conducted by CMS program integrity contractors and to deny improper payments. In developing leads, FPS is intended to help CMS avoid improper payment costs by enabling quicker investigations and more timely corrective actions. Additionally, in 2012, CMS helped establish the HFPP to collaborate with other health care payers to address health care fraud. One of the key activities of the HFPP is to analyze claims data that are pooled from multiple payers, including private payers and Medicare.

GAO was asked to review CMS's use of FPS and the activities of the HFPP. This report examines 1) CMS's use of FPS to identify and investigate providers suspected of potential fraud, 2) the types of payments that have been denied by FPS, and 3) HFPP efforts to further CMS's and payers' ability to address health care fraud. GAO reviewed CMS documents, including reports to Congress on FPS, contractor statements of work, and information technology system user guides, and obtained fiscal year 2015 and 2016 data on FPS fraud investigations and claim denials. GAO also interviewed CMS officials and CMS program integrity contractors regarding how they use FPS, and a non-generalizable selection of HFPP participants regarding information and data sharing practices, and anti-fraud collaboration efforts.

View GAO-17-710. For more information, contact Kathleen M. King at (202) 512-7114 or kingk@gao.gov.

What GAO Found

Investigations initiated or supported by the Centers for Medicare & Medicaid Services' (CMS) Fraud Prevention System (FPS)—a data analytic system—led to corrective actions against providers and generated savings. For example, in fiscal year 2016, CMS reported that 90 providers had their payments suspended because of investigations initiated or supported by FPS, which resulted in an estimated $6.7 million in savings. In fiscal year 2016, 22 percent of Medicare fraud investigations conducted by CMS program integrity contractors were based on leads generated by FPS analysis of Medicare claims data. Officials representing Medicare's program integrity contractors told GAO that FPS helps speed up certain investigation processes, such as identifying and triaging suspect providers for investigation. However, the officials said that once an investigation is initiated, FPS has generally not sped up the process for investigating and gathering evidence against suspect providers. CMS has not tracked data to assess the extent to which FPS has affected the timeliness of contractor investigation processes. However, CMS is implementing a new information technology system that tracks such data, and officials said that they plan to use the data to assess FPS's effect on timeliness.

FPS denies individual claims for payment that violate Medicare rules or policies through prepayment edits—automated controls that compare claims against Medicare requirements in order to approve or deny claims. FPS prepayment edits specifically target payments associated with potential fraud. For example, an FPS edit denies physician claims that improperly increase payments by misidentifying the place that the service was rendered, which helped address a payment vulnerability associated with millions in overpayments. FPS edits do not analyze individual claims to automatically deny them based on risk alone or the likelihood that they are fraudulent without further investigation. As of May 2017, CMS had implemented 24 edits in FPS. CMS reported that FPS edits denied nearly 324,000 claims and saved more than $20.4 million in fiscal year 2016.

The Healthcare Fraud Prevention Partnership (HFPP) is a public-private partnership that began in 2012 with the aim of facilitating collaboration among health care payers to address health care fraud. The HFPP had 79 participants as of June 2017. Participants, including CMS officials, stated that sharing data and information within HFPP has been useful to their efforts to address health care fraud. HFPP conducts studies that pool and analyze multiple payers' claims data to identify providers with patterns of suspect billing across payers. Participants reported that HFPP's studies helped them to identify and take action against potentially fraudulent providers and payment vulnerabilities of which they might not otherwise have been aware. For example, one study identified providers who were cumulatively billing multiple payers for more services than could reasonably be rendered in a single day. Participants also stated that HFPP has fostered both formal and informal information sharing among payers.

The Department of Health and Human Services provided technical comments on a draft of this report, which GAO incorporated as appropriate.

Contents

Letter 1

Background 4
CMS Program Integrity Contractors Reported That FPS Speeds Up Certain Investigation Processes and Has Contributed to Program Savings 12
FPS Denies Payments Based on Medicare Rules or Policies and Not Fraud Risk 18
Participants Reported That HFPP Efforts Furthered Their Ability to Address Health Care Fraud 20
Agency Comments 24

Appendix I: GAO Contact and Staff Acknowledgments 27

GAO Contact 27
Staff Acknowledgments 27

Tables

Table 1: Administrative Actions Against Medicare Providers That May Result from Program Integrity Investigations 9
Table 2: Sources of Zone Program Integrity Contractor (ZPIC) Investigations, Fiscal Years (FY) 2015 and 2016 14
Table 3: CMS Reported Program Integrity Contractor Corrective Actions and Associated Savings from FPS, Fiscal Years (FY) 2015 and 2016 16
Table 4: Healthcare Fraud Prevention Partnership Completed Studies as of May 2017 21

Figures

Figure 1: Zone Program Integrity Contractor (ZPIC) and Unified Program Integrity Contractor (UPIC) Jurisdictions 7
Figure 2: Program Integrity Contractor Investigation Processes 8
Figure 3: Medicare Claims Processing 11

Abbreviations

CMS	Centers for Medicare & Medicaid Services
CPI	Center for Program Integrity
FPS	Fraud Prevention System
HFPP	Healthcare Fraud Prevention Partnership
HHS	Department of Health and Human Services
HHS OIG	Department of Health and Human Services Office of Inspector General
IT	information technology
MAC	Medicare Administrative Contractor
TTP	trusted third party
UPIC	Unified Program Integrity Contractor
ZPIC	Zone Program Integrity Contractor

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

August 30, 2017

Congressional Requesters

In fiscal year 2016, Medicare provided health insurance for approximately 57 million elderly and disabled beneficiaries at a cost of approximately $699 billion.[1] Since 1990, we have designated Medicare a high-risk program because of its size, complexity, and susceptibility to mismanagement and improper payments.[2] Some improper Medicare payments are due to fraud, which involves willful misrepresentation.[3] Although the deceptive nature of fraud makes its extent in the Medicare program difficult to measure in a reliable way, there have been convictions for multimillion dollar schemes defrauding the program.

The Centers for Medicare & Medicaid Services (CMS)—the agency within the Department of Health and Human Services (HHS) that administers the Medicare program—is responsible for conducting program integrity activities intended to reduce fraud, waste, and abuse. CMS uses analyses of claims submitted for payment by health care providers as part

[1]Medicare is the federally financed health insurance program for persons aged 65 and over, certain individuals with disabilities, and individuals with end-stage renal disease. Medicare Part A covers inpatient hospital services, skilled nursing facility services, some home health services, and hospice services. Medicare Part B covers physician and hospital outpatient services, and durable medical equipment, prosthetics, orthotics, and supplies, among other things. Together, Parts A and B are known as traditional Medicare or Medicare fee-for-service.

[2]See GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

[3]The Medicare fee-for-service program generally makes payments directly to health care providers, such as hospitals and physicians. An improper payment is any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. This includes any payment to an ineligible recipient, any payment for an ineligible good or service, any duplicate payment, any payment for a good or service not received (except for such payments where authorized by law), and any payment that does not account for credit for applicable discounts. Improper payments may be a result of fraud, waste, or abuse. Fraud involves an intentional act or representation to deceive with the knowledge that the actions or representation could result in gain. Whether an act is in fact fraud is a determination that is made through the judicial or other adjudicative system. Waste includes overusing services, such as excessive diagnostic testing. Abuse involves actions inconsistent with acceptable business or medical practices.

of its program integrity activities. In 2011, CMS implemented a data analytic system—the Fraud Prevention System (FPS)—that analyzes Medicare fee-for-service claims to identify health care providers with suspect billing patterns for further investigation and to prevent improper payments. Additionally, in 2012, HHS helped establish a public-private partnership—the Healthcare Fraud Prevention Partnership (HFPP)—with other health care payers, agencies, and organizations to address healthcare fraud. One of the key activities of HFPP is analyzing claims data pooled from multiple payers, including Medicare, to identify and disseminate information within the partnership on providers with suspect billing patterns.

You asked us to review CMS's use of FPS and the activities of HFPP. This report examines

1. CMS's use of FPS to identify and investigate providers suspected of potential fraud;
2. the types of payments that have been denied by FPS; and
3. HFPP's efforts to further CMS's and payers' ability to address health care fraud.

To examine CMS's use of FPS to identify and investigate suspect providers, we reviewed CMS documents, including CMS reports to Congress on FPS's implementation, statements of work for program integrity contractors, and FPS and other CMS information technology (IT) system user guides. We interviewed CMS officials and officials from all seven Zone Program Integrity Contractors (ZPIC)—the contractors responsible for identifying and investigating potential Medicare fraud, waste, and abuse—regarding how FPS is used to identify and investigate potential fraud.[4] CMS is currently in the process of transitioning Medicare program integrity contracts from ZPICs to new contract entities, Unified Program Integrity Contractors (UPIC), and we interviewed officials from the two UPICs in operation as of May 2017.[5] We also obtained and

[4]CMS began implementing ZPICs in 2008 to replace legacy program integrity contractors, Program Safeguard Contractors. Program Safeguard Contractors continued to operate in one ZPIC jurisdiction— Zone 6—because of protest-related delays with the Zone 6 ZPIC contract. We interviewed officials representing the Program Safeguard Contractors that operated in Zone 6. For the sake of simplicity, references to ZPICs in this report are inclusive of the Zone 6 Program Safeguard Contractors.

[5]UPICs combine responsibility for conducting program integrity activities for both the Medicare and Medicaid programs. CMS plans to award all UPIC contracts by the end of calendar year 2017.

analyzed fiscal year 2015 and 2016 data from CMS on the sources of ZPIC investigations and the corrective actions and savings associated with ZPIC investigations. To assess the reliability of the data, we reviewed relevant agency documents, interviewed CMS officials, compared the data to published data, and reviewed the data for any outliers and obvious errors. We found the data sufficiently reliable for the purposes of our study.

To examine the types of payments that have been denied by FPS, we obtained information from CMS on the prepayment edits—automated controls that compare claim information to Medicare coverage and payment policies in order to approve or deny claims—that have been implemented in FPS.[6] We interviewed CMS officials about how FPS's edits identify and deny payments. We also interviewed officials representing Medicare Administrative Contractors (MAC)—the contractors that process and pay Medicare fee-for-service claims and, along with CMS, are responsible for implementing prepayment edits—regarding differences between edits in FPS and those in Medicare's claims processing systems. In addition, we obtained data from CMS on the number of claims denied by FPS edits and the associated savings for fiscal years 2015 and 2016. To assess the reliability of the data, we interviewed CMS officials, compared the data to published data, and reviewed the data for any outliers and obvious errors. We found the data sufficiently reliable for the purposes of our study.

To examine HFPP's efforts to further CMS's and payers' ability to address health care fraud, we reviewed CMS and HFPP documents, including HFPP study summaries and findings. We interviewed officials from CMS and the contractors that have administered HFPP about HFPP information and data sharing practices. We also interviewed a non-generalizable selection of HFPP participants that reflect HFPP's membership. We interviewed officials representing 3 private payers, 5 state agencies, and 4 associations regarding HFPP's anti-fraud collaboration efforts. We selected private payers that offer Medicare Advantage plans, state agencies that use data analytic systems or have shared data for HFPP studies, and healthcare and healthcare fraud specific associations.

[6]References to FPS claim denials refer to both claims that are rejected or denied by the system. Claims that are rejected can be corrected and resubmitted, while claims that are denied cannot be resubmitted.

We conducted this performance audit from April 2016 to August 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Fraud Prevention System

To advance CMS's efforts to prevent fraud, waste, and abuse in the Medicare fee-for service program, the Small Business Jobs Act of 2010 appropriated $100 million for CMS to implement a data analytic system.[7] The law required CMS to implement a system that could analyze claims prior to payment to identify suspect claims and provider billing patterns and prevent payment of improper and potentially fraudulent claims, among other things. In April 2011, CMS awarded almost $77 million to a contractor to implement, operate, and maintain FPS and design analytic models for the system. CMS awarded about $13 million to a second contractor in July 2011 to develop additional analytic models for FPS. As the original FPS contract was set to end, CMS awarded a nearly $92 million contract in April 2016 for a new, upgraded FPS system—FPS 2.0. FPS 2.0 was fully implemented in March 2017.

CMS's Center for Program Integrity (CPI)—which oversees the agency's Medicare program integrity efforts—employs FPS as a key component of its strategy to move beyond the "pay and chase" approach of recovering improper and potentially fraudulent payments to focusing on prevention. FPS screens fee-for-service claims prior to payment in order to help

[7]A portion of the appropriated funds was required to be used for an independent evaluation of the program. Pub. L. No. 111-240, § 4241(h), 124 Stat. 2504, 2603 (2010) (codified at 42 U.S.C. § 1320a-7m(h)). Data analytic systems are IT systems that use a variety of techniques to analyze and interpret data to facilitate decision making, and can be used to identify patterns or trends. We have previously reported on the importance of agencies using data analysis to manage fraud risks. See GAO, *A Framework for Managing Fraud Risks in Federal Programs*, GAO-15-593SP (Washington, D.C.: July 2015) and GAO, *Highlights of a Forum: Data Analytics to Address Fraud and Improper Payments*, GAO-17-339SP (Washington, D.C.: Mar. 31, 2017).

identify and prevent improper and potentially fraudulent payments by performing two primary functions:

- *Develop leads for fraud investigations*. FPS compares provider billing patterns and other data against models of potentially fraudulent behavior to identify providers with suspect billing patterns. For example, an FPS model identifies providers that bill for a disproportionate number of services in a single day relative to other providers. FPS simultaneously risk-scores providers identified by the models to prioritize them for potential investigation. In developing these leads, FPS is intended to help CMS prevent potentially fraudulent payments by furthering the agency's ability to more quickly identify and investigate suspect providers, and take more timely corrective actions.
- *Execute automated prepayment edits*. FPS edits deny certain improper payments, and some edits compare information from multiple claims to do so. For example, FPS may deny physician outpatient claims based on information from an inpatient claim associated with the same episode of care.

CMS submitted three annual reports on FPS's implementation to Congress in response to requirements established by the Small Business Jobs Act of 2010. In these reports, CMS provided information on the corrective actions taken and savings achieved from FPS.[8] In its most recent report, CMS reported that FPS had cumulatively helped prevent or identify nearly $1.5 billion in improper and potentially fraudulent payments from its implementation through the end of calendar year 2015.[9]

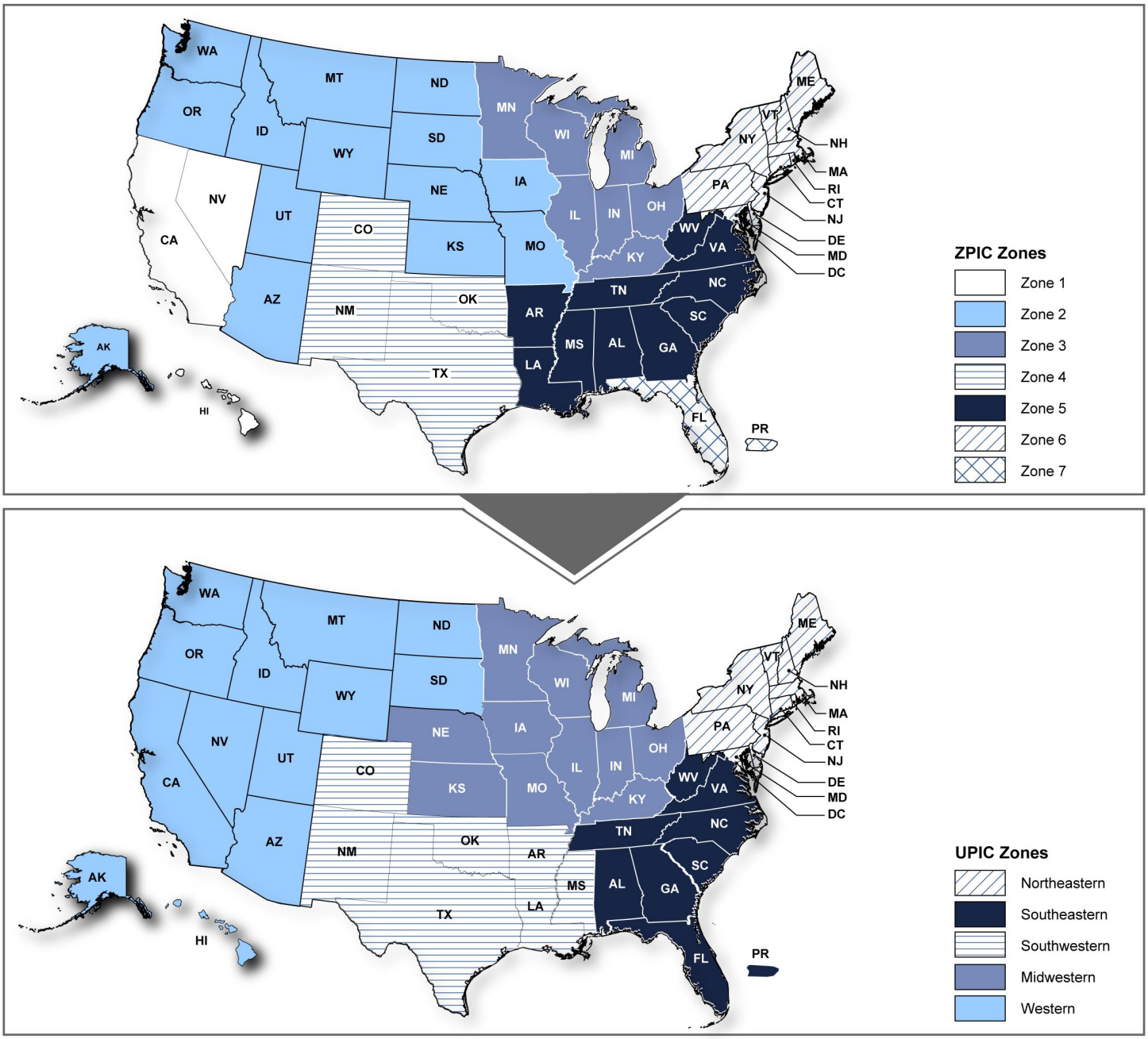
[8]The act further required HHS Office of Inspector General (HHS OIG) to certify the reported savings from FPS, and HHS OIG issued companion reports on CMS's reported savings for the first three years of FPS. Although not required by the act to report on FPS after the first three years, CMS publicly issued a fourth year report. See https://www.cms.gov/About-CMS/Components/CPI/Downloads/Fraud-Prevention-System-Return-on-Investment-Fourth-Implementation-Year-2015.pdf

[9]The $1.5 billion figure above includes both payments directly prevented by FPS, such as prepayment edit claim denials, and identified savings associated with actions taken against providers suspected of fraud, such as the amount of overpayments referred for collection. The actual savings achieved is lower because of a number of factors. For example, not all referred overpayments can be recovered. CMS applies adjustment factors to the identified savings to estimate actual savings from FPS. For instance, while CMS reported $454 million in prevented and identified savings from FPS in calendar year 2014, CMS estimated actual savings of $133 million. For more information on the adjustment factors used by CMS, see CMS, *Report to Congress Fraud Prevention System Second Implementation Year*, June 2014.

Medicare Program Integrity

CMS uses contractors to support the agency's program integrity activities, including program integrity contractors to identify and investigate providers engaged in potential Medicare fee-for-service fraud. CMS is currently in the process of transitioning Medicare program integrity contracts from ZPICs to new contract entities, UPICs. ZPICs operated in seven geographical jurisdictions across the country. UPICs will operate in five jurisdictions and combine Medicare and Medicaid program integrity efforts under a single contracting entity (fig. 1 depicts the geographic jurisdictions of ZPIC and UPIC zones). As of May 2017, two of the five UPICs—the Midwestern and Northeastern—were operational.

Figure 1: Zone Program Integrity Contractor (ZPIC) and Unified Program Integrity Contractor (UPIC) Jurisdictions



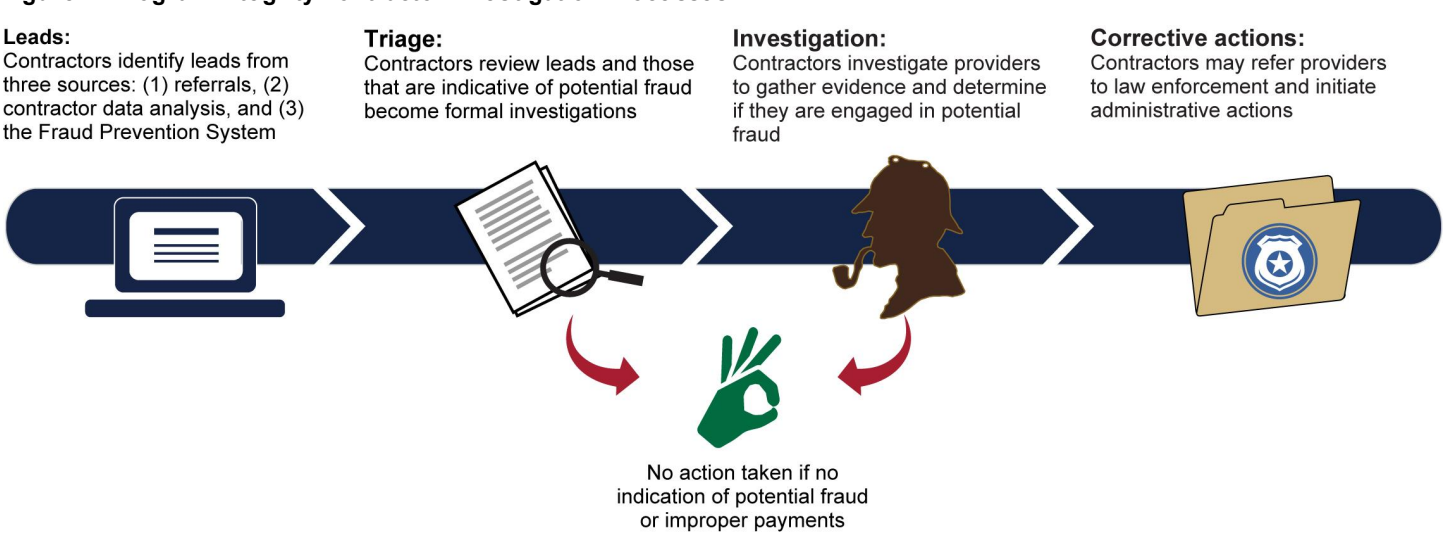
Sources: CMS; Map Resources (map). | GAO-17-710

The program integrity contractors identify leads for provider investigations from three categories of sources:

- *Referrals.* A number of entities, including CMS, law enforcement agencies, and the MACs, refer leads about suspect providers to the program integrity contractors. The program integrity contractors also receive leads based on beneficiary and provider complaints and allegations.
- *Program integrity contractor data analysis*. Program integrity contractors use postpayment claims to conduct their own data analyses to identify providers with suspect billing patterns.
- *FPS.* FPS identifies providers with suspect billing patterns and prioritizes leads based on provider risk-scores.

The program integrity contractors generally have a triage process to review leads and determine whether the leads are indicative of potential fraud (see fig. 2 for information on program integrity contractor investigation processes). Leads that are determined to be suspect become formal investigations, and the program integrity contractors perform a range of investigative activities to gather evidence and determine if providers are engaged in potential fraud. These activities include conducting beneficiary and provider interviews, site visits of provider facilities, and manual reviews of provider claims.

Figure 2: Program Integrity Contractor Investigation Processes



Source: GAO analysis of CMS information. | GAO-17-710

Based on their investigations, the program integrity contractors may take corrective actions by referring providers engaged in potential fraud to law enforcement and initiating administrative actions. Specifically, if the program integrity contractors uncover evidence of potential fraud, they

refer the investigation to the Department of Health and Human Services Office of Inspector General (HHS OIG) for further examination, which may lead to possible criminal or civil prosecution by the Department of Justice. The program integrity contractors may also recommend a range of administrative actions to CMS for approval and implementation. Such actions include revocation of providers' billing privileges and payment suspensions (table 1 describes the administrative actions the program integrity contractors may recommend against providers).

Table 1: Administrative Actions Against Medicare Providers That May Result from Program Integrity Investigations

Action	Definition
Prepayment review	Provider-specific prepayment edits that suspend payments pending manual claim review.
Provider-specific auto-denial edits	Provider-specific prepayment edits that automatically deny payments to the provider.
Payment suspension	Temporary suspension of provider payments pending investigation of potential fraud.
Overpayment determination	Referral for collection of provider payments received in excess of amounts due and payable.
Revocation	Termination of provider's billing privileges.

Source: GAO analysis of CMS information. | GAO-17-710

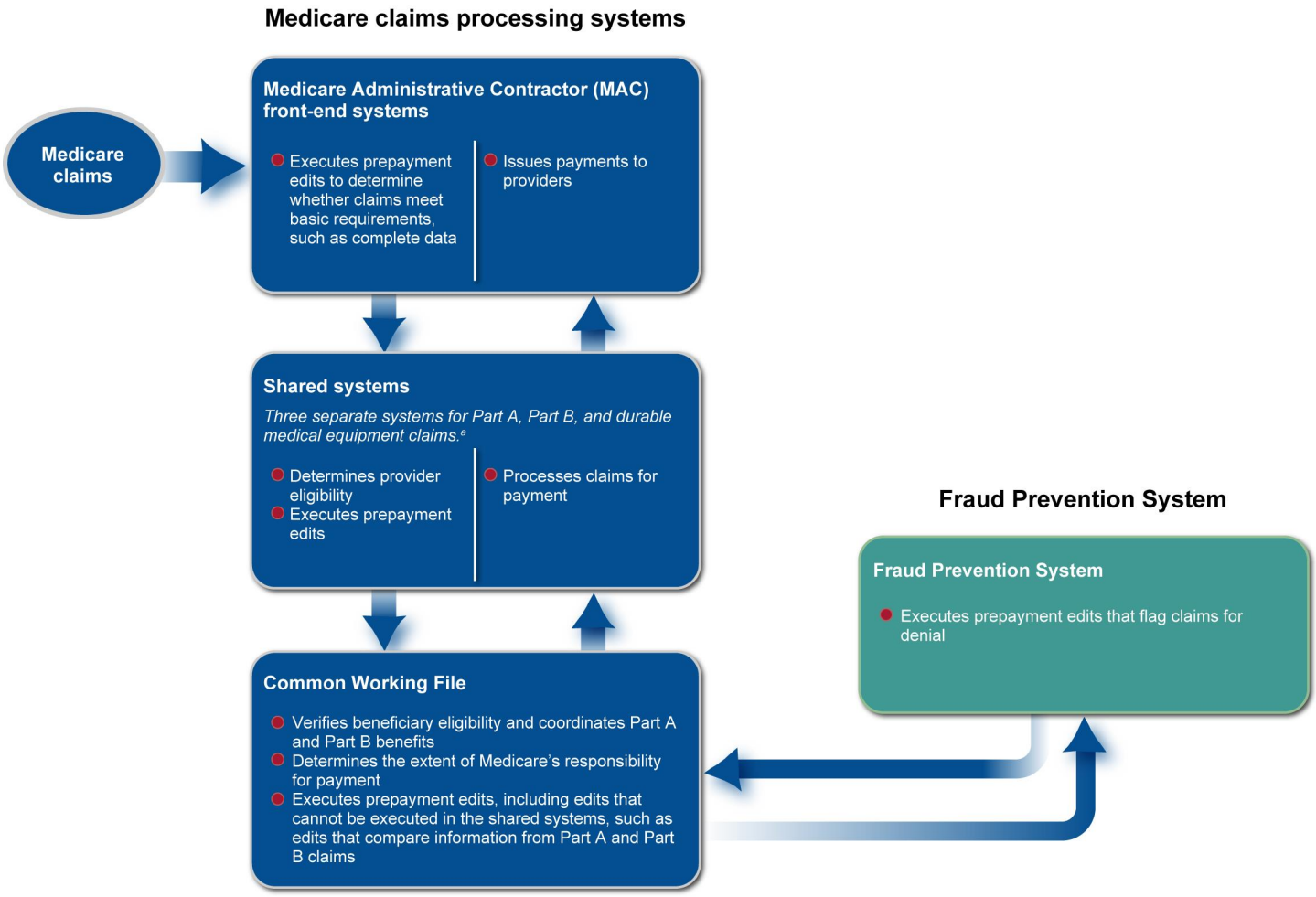
CMS's Prepayment Edits Process

CMS's claims processing systems apply prepayment edits to all Medicare fee-for-service claims in an effort to pay claims properly. Most of the prepayment edits are automated, meaning that if a claim does not meet the criteria of the edit, it is automatically denied. Other prepayment edits flag claims for manual review, in which trained clinicians and coders examine claims and associated medical records to ensure that the claims meet Medicare rules and requirements. Many improper and potentially fraudulent claims can be identified only by manually reviewing associated medical records and beneficiary claim histories, and exercising clinical judgment to determine whether services were reasonable and necessary. Whereas automated edits are applied to all claims, manual edits are applied to very few—less than 1 percent of claims undergo manual review.

CMS contracts with the MACs to process and pay Medicare fee-for-service claims and implement prepayment edits in the Medicare claims processing systems.[10] The claims processing systems consist of three systems—the MAC front-end systems, shared systems, and Common Working File—that carry out a variety of functions and execute prepayment edits (see fig. 3). When implementing FPS, CMS integrated FPS with the claims processing systems and claims are screened by FPS prior to payment. Unlike the claims processing systems, CPI maintains FPS.

[10]CMS is generally required to pay Medicare claims between 14 and 30 days from the date of receipt.

Figure 3: Medicare Claims Processing



Source: GAO analysis of CMS information. | GAO-17-710

[a]The shared systems are the Fiscal Intermediary Shared System, Multi-Carrier System, and the ViPS Medicare System. The Fiscal Intermediary Shared System processes Part A claims and certain Part B claims related to medical care provided by institutional providers, such as hospital inpatient and outpatient departments. The Multi-Carrier System processes all other Part B claims, such as physician claims. The ViPS Medicare System processes claims for durable medical equipment.

Healthcare Fraud Prevention Partnership

HFPP is a voluntary public-private partnership established by HHS and the Department of Justice to facilitate collaboration in addressing healthcare fraud. The membership includes Medicare- and Medicaid-related federal agencies and several state agencies, other federal agencies with responsibility for federal health care programs such as the

Department of Defense and Department of Veterans Affairs, law enforcement agencies, private payers, and antifraud and other healthcare organizations. HFPP was established, in part, to help payers identify schemes and providers engaged in potential fraud that individual payers may not be able to identify alone. HFPP began in 2012 with 20 members and, as of June 2017, had grown to 79 members.[11] As of the end of calendar year 2016, CMS had cumulatively spent $30.3 million on HFPP.

CMS Program Integrity Contractors Reported That FPS Speeds Up Certain Investigation Processes and Has Contributed to Program Savings

CMS Program Integrity Contractors Reported That FPS Speeds Up Certain Investigation Processes, and CMS Is Taking Steps to Track Data on Timeliness

ZPIC officials stated that FPS helps them identify suspect providers quickly. Because FPS analyzes claims prior to payment, providers with suspect billing patterns can be identified quickly relative to other sources of leads. In particular, several ZPIC officials stated that the leads they develop from their data analyses of postpayment claims are not as timely. Officials from two ZPICs estimated that the postpayment claims they use for their analyses may have been for services rendered 1 to 2 months prior, while the claims analyzed by FPS may have been for services recently rendered.

ZPIC officials also said the information associated with FPS leads allows them to examine and triage those leads quickly to determine whether to initiate investigations. FPS leads provide specific information about the type of potential fraud identified, along with claims data and other supporting information. ZPIC officials further stated that they use

[11]In November 2016, HFPP had 70 members and CMS reported that payer participants covered approximately 65 percent of covered U.S. individuals.

information from FPS when triaging leads from other sources. In contrast to FPS leads, several ZPIC officials noted that reviewing and triaging leads based on referrals often necessitates additional time and resources. In particular, allegations associated with some referrals can be vague, which makes it difficult for ZPICs to identify the relevant provider claims data and other information needed to assess the validity of the allegations.

However, once an investigation is initiated, officials stated that FPS has generally not sped up the process for investigating providers. Several ZPIC officials noted that investigations based on FPS leads are similar to those from other sources in that they require further investigation, such as manual claim reviews or site visits of provider facilities, to substantiate the leads and gather evidence of potential fraud. However, while ZPIC officials said that FPS does not speed up investigations, officials from several ZPICs noted that FPS can help improve the quality of beneficiary interviews. Since FPS leads are based on prepayment claims data, ZPICs can conduct beneficiary interviews shortly after the services have been rendered, when beneficiaries may be better able to recall details about their care.

CMS has not tracked data to assess FPS's effect on the timeliness of investigation processes.[12] CMS has lacked such timeliness data because of limitations with its IT system for managing and overseeing ZPICs. However, as of May 2017, CMS was in the process of implementing a new IT system that could be used to assess FPS's effect on the timeliness of program integrity contractor investigation processes. In transitioning to UPICs, CMS is implementing a new contractor workload management system that will capture data on the timeliness of UPIC investigation processes.[13] For example, the system will be able to capture information on the amount of time it takes a UPIC to evaluate a lead or conduct an investigation. CMS officials said that the agency plans to use the information tracked by the system to monitor program performance, including assessing FPS's effect on UPIC investigation processes and the

[12]We previously reported on the importance of tracking the timeliness of program integrity contractor investigation processes, since CMS can save money by taking administrative actions against providers suspected of fraud more quickly. See GAO, *Medicare Program Integrity: Contractors Reported Generating Savings, but CMS Could Improve Its Oversight*, GAO-14-111 (Washington, D.C.: Oct. 25, 2013).

[13]CMS is replacing the Analysis, Reporting, and Tracking system used by ZPICs with the Unified Case Management system for UPICs.

timeliness of corrective actions. The officials also stated that they may not be able to conduct such an assessment for several years as CMS is still in the process of transitioning to UPICs and implementing the new IT system. Further, the officials said that they subsequently would want to collect several years' worth of such data to ensure a reliable assessment.

FPS Accounted for About 20 Percent of Investigations in 2015 and 2016 and Contributed to Program Savings

In fiscal years 2015 and 2016, about 20 percent of ZPIC investigations were initiated based on FPS leads, according to our analysis (see table 2). In both years, nearly half of ZPIC investigations were based on referrals.

Table 2: Sources of Zone Program Integrity Contractor (ZPIC) Investigations, Fiscal Years (FY) 2015 and 2016

	FY 2015		FY 2016	
Source of investigations	Number of new investigations	Percentage of workload	Number of new investigations	Percentage of workload
Referrals	1513	53	1395	47
ZPIC data analysis	722	25	937	31
FPS	604	21	654	22

Source: GAO analysis of CMS data. | GAO-17-710

Note: Percentages may not sum to 100 due to rounding.

The proportion of investigations based on FPS leads is poised to increase as CMS changes program integrity contractor requirements for using FPS with the transition from ZPICs to UPICs. CMS has required the ZPICs to review all FPS leads that met high-risk thresholds. CMS is instead requiring that the UPICs derive 45 percent of new investigations from FPS. ZPIC officials stated that the new UPIC requirement should allow UPICs flexibility to focus their reviews on the FPS leads that are most applicable to their geographic region. For example, a UPIC with high

levels of home health agency fraud within its jurisdiction can focus its reviews of FPS leads on those providers.[14]

Investigations initiated by FPS and existing investigations that were supported by FPS have led to corrective actions against providers engaged in potential fraud and program savings, based on CMS reported data. For example, in fiscal year 2015, nearly 60 percent of providers subject to prepayment review and 25 percent of estimated savings from prepayment reviews were associated with FPS (see table 3). In fiscal year 2016, nearly 25 percent of provider payment suspensions and about 15 percent of estimated savings from payment suspensions were associated with FPS.

[14]We previously found CMS's requirement that ZPICs review all FPS leads that met high-risk thresholds created challenges for ZPICs because FPS sometimes prioritized leads that targeted fraud schemes that were not prevalent in specific ZPIC zones. See GAO, *Medicare Fraud Prevention: CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness*, GAO-13-104 (Washington, D.C.: Oct. 15, 2012).

Table 3: CMS Reported Program Integrity Contractor Corrective Actions and Associated Savings from FPS, Fiscal Years (FY) 2015 and 2016

	FY 2015			FY 2016		
Action	**Total actions**	**Actions associated with FPS[a]**	**Percentage associated with FPS**	**Total actions**	**Actions associated with FPS[a]**	**Percentage associated with FPS**
Number of providers subject to prepayment review	546	311	57%	686	446	65%
Estimated savings[b] (dollars in millions)	$59.8	$15.0	25%	$54.0	$17.3	32%
Number of providers subject to auto-denial edits[c]	—	236	—	—	238	—
Estimated savings[b] (dollars in millions)	$63.4	$1.5	2%	$54.5	$1.7	3%
Number of overpayment determinations referred for collection	876	443	51%	1112	526	47%
Amount referred for collection (dollars in millions)	$935.7	$291.7	31%	$1221.2	$358.8	29%
Estimated savings[d] (dollars in millions)	$175.5	$40.0	23%	$178.7	$52.7	29%
Number of providers subject to payment suspension during the fiscal year	377	55	15%	393	90	23%
Estimated savings[e] (dollars in millions)	$49.7	$12.9	26%	$46.7	$6.7	14%
Number of providers revoked	441	101	23%	303	45	15%
Number of providers referred to law enforcement[f]	—	53	—	—	41	—

Source: GAO analysis of Centers for Medicare & Medicaid Services (CMS) data. | GAO-17-710

Notes: CMS applies adjustment factors to identified savings amounts to estimate actual savings. For more information on the adjustment factors used by CMS, see CMS, Report to Congress Fraud Prevention System Second Implementation Year, June 2014.

[a]Includes both actions from investigations initiated by the Fraud Prevention System (FPS) and existing investigations that were supported or corroborated by FPS.

[b]The savings amounts are estimates of what CMS would have paid had the claims been processed, and are further adjusted based on the historic rate at which claim denials are overturned on appeal.

[c]For the total actions, CMS tracked the number of auto-denial edits implemented. For actions associated with FPS, CMS tracked the number of providers subject to auto-denial edits. These data are not directly comparable.

[d]The savings amounts are estimates based on historic overpayment collection rates, with the exception of the total amount collected in FY 2016. Starting in FY 2016, CMS began tracking total overpayment savings based on actual amounts collected.

[e]The savings amounts are estimates based on the historic rate at which payments held in suspension because of program integrity contractor actions are later recouped.

[f]For total actions, CMS tracked the number of investigations referred to law enforcement. For actions associated with FPS, CMS tracked the number of providers referred to law enforcement. These data are not directly comparable.

In addition to tracking the corrective actions and savings associated with FPS, CMS also measures the extent to which investigations initiated from FPS leads result in actions against providers engaged in potential fraud.[15] CMS reported that, in fiscal year 2015, 44 percent of FPS-initiated investigations resulted in administrative actions, which met the agency's fiscal year goal of 42 percent of investigations leading to administrative actions. In fiscal year 2016, 38 percent of FPS-initiated investigations resulted in administrative actions, which did not meet the agency's fiscal year goal of 45 percent.

[15]CMS developed this measure in response to a prior GAO recommendation that the agency develop outcome-based performance goals to measure FPS's performance. See GAO-13-104.

FPS Denies Payments Based on Medicare Rules or Policies and Not Fraud Risk

FPS prepayment edits screen individual claims to automatically deny payments that violate Medicare rules or policies. For example, some FPS edits deny claims that exceed coverage utilization limits for a service. FPS edits do not analyze individual claims to automatically deny payments based on risk alone or the likelihood that they are fraudulent.[16] According to CMS officials, the agency does not have the authority to use FPS to automatically deny individual claims based on risk without further evidence confirming that the claims are potentially fraudulent.[17]

Although the prepayment edits in FPS are functionally similar to those in CMS's claims processing systems, the FPS edits specifically target payments associated with potential fraud schemes. Like edits executed elsewhere in the claims processing systems, FPS edits deny payments based on rules or policies. Unlike the edits in the claims processing systems, all of the edits in FPS are designed to address identified payment vulnerabilities associated with potential fraud, according to CMS officials. Payment vulnerabilities are service- or system-specific weaknesses that can lead to improper payments, including improper payments that may be due to fraud. For example, CMS implemented an FPS edit that denies physician claims that improperly increase payments by misidentifying the location that the service was rendered. The payments are denied based on the rule that physician claims must correctly identify the place of service. The edit helped address a payment

[16]We previously analyzed the use of analytic systems by health care payers and did not identify any payers that use analytic systems to automatically deny individual claims based on the likelihood that they are fraudulent. See GAO-13-104.

[17]CMS may suspend payment based on reliable information of an overpayment, or pending an investigation of a credible allegation of fraud as determined in consultation with HHS OIG. 42 U.S.C. § 1395y(o); 42 C.F.R. § 405.371 (2016). CMS program integrity activities intended to address fraud generally do not focus on reviewing whether individual payments are potentially fraudulent, but instead focus on identifying suspect billing patterns and taking action against providers engaged in potential fraud. Payment denials of potentially fraudulent claims generally stem from investigations into or corrective actions taken against providers, such as payments denied for providers subject to prepayment review.

vulnerability identified by HHS OIG that found millions of dollars in overpayments.[18]

According to CMS officials, the advantage of using FPS to implement prepayment edits is that the system allows CMS to prioritize edits intended to address payment vulnerabilities associated with potential fraud. Because CPI maintains FPS, CMS can quickly implement edits into FPS. In contrast, edits that are implemented in the claims processing systems are queued as part of quarterly system updates, and may need to compete with other claims processing system updates. CPI is not subject to such limitations when implementing edits in FPS, and officials said that edits can be developed and implemented in FPS more quickly compared to the claims processing systems.

As of May 2017, CMS had implemented 24 edits in FPS. CMS reported that in fiscal year 2015, FPS edits denied nearly 169,000 claims and saved $11.3 million. In fiscal year 2016, the edits denied nearly 324,000 claims and saved $20.4 million.[19] CMS officials stated that the number of prepayment edits implemented in FPS thus far has been limited, but that the agency is taking steps to address certain challenges that would allow the agency to develop and implement edits more quickly. For example, because of their role and expertise in processing claims, the MACs advise CPI and help develop and test FPS edits before they are implemented in the system to ensure they will work as intended. However, CPI has been limited in the amount of MAC resources that it can engage to help develop FPS edits under existing contracts. According to officials, CPI is planning to take steps to more directly involve the MACs in FPS edit development, which officials said should accelerate the edit implementation process. Additionally, CMS officials

[18]Medicare payments to physicians account for overhead expenses. HHS OIG found physician claims for services performed at facility locations, such as ambulatory surgical centers, that were billed as if they had been performed at physician offices. This resulted in overpayments to physicians for office overhead expenses. See Department of Health and Human Services Office of Inspector General, *Incorrect Place-of-Service Claims Resulted in Potential Medicare Overpayments Costing Millions*, A-01-13-00506 (Washington, D.C.: May 2015).

[19]As of the end of fiscal year 2016, CMS had implemented 17 edits, and officials told us that 7 additional edits have since been added. CMS reported that in fiscal year 2015, FPS edits denied $17.5 million and, in fiscal year 2016, denied $33.6 million. The savings data above excludes payments associated with denied claims that were later corrected, resubmitted, and paid, and amounts associated with resubmitted claims that were again denied by FPS.

said that they plan to utilize FPS functionality to implement new edits by expanding existing edits to apply to other services. All of the 24 current FPS edits were developed from the ground up, a time and resource consuming process, according to CMS officials. In contrast, developing new edits by expanding existing edits will allow CMS to more quickly develop and implement new edits.

Participants Reported That HFPP Efforts Furthered Their Ability to Address Health Care Fraud

Participants Reported That Information Sharing through HFPP Furthered Efforts to Address Fraud

HFPP participants we interviewed, including CMS officials, reported that sharing data and information within HFPP has been useful to their efforts to address health care fraud. The principal activity of HFPP is generating studies that pool and analyze multiple payers' claims data to identify providers with patterns of suspect billing across multiple payers. Study topics examine known fraud vulnerabilities important to the participating payers and are selected through a collaborative process. As an example, one study used pooled data to identify providers who were cumulatively billing multiple payers for more services than could reasonably be rendered in a single day. In another study, HFPP pooled payer information on billing codes that are frequently misused by providers engaged in potential fraud, such as codes commonly used to misrepresent non-covered services as covered. See table 4 for a description of HFPP's completed studies as of May 2017.

Table 4: Healthcare Fraud Prevention Partnership Completed Studies as of May 2017

Study	Description
Misused Codes and Fraud Schemes	A pooled list of approximately 1400 misused codes and 100 fraud schemes.
Non-Operational Providers	A pooled list of providers that have been found to be non-operational, such as false store fronts, and only exist on paper to file claims for services that were never rendered.
Revoked/Terminated Providers	A pooled list of provider organizations that have been revoked or terminated by payers for reasons relating to fraud, waste, and abuse.
Top Billing Pharmacies for Controlled Prescription Drugs	An analysis identifying the billing pharmacies with extreme outlier dispensing of controlled prescription drugs.
Urine Drug and Genetic Testing Referrals	An analysis identifying providers with unusual referral patterns for urine drug and genetic testing.
Psycho-Therapy Timed Code Analysis	An analysis of behavioral health providers identifying those who may be cumulatively billing multiple payers for more services than could reasonably be rendered in a single day.

Source: GAO analysis of CMS information. | GAO-17-710

Participants reported that HFPP's studies helped them to identify and take action against potentially fraudulent providers that would otherwise have gone unidentified. For instance, both public and private payers reported that HFPP's non-operational providers report uncovered providers that they had not previously identified as suspect. CMS officials and one private payer we interviewed said that they used information from this study to conduct site visits of reportedly non-operational providers. CMS officials told us that they revoked a number of the providers after confirming that they were indeed non-operational. CMS officials also said that they review the results of HFPP studies and provide information on potentially fraudulent providers to ZPICs when appropriate. The information may either serve as new leads or help support existing investigations.

Participants also reported that study results have helped them uncover payment vulnerabilities of which they might not otherwise have been aware. For example, CMS officials stated that they used the HFFP report on misused procedure codes to evaluate several Medicare payment vulnerabilities and then implemented edits to address them. In instances where participants reported that HFPP studies revealed suspect providers or schemes that were known to them, participants stated that HFPP study

results helped them to confirm suspicions, better assess potential exposure, and prioritize and develop internal investigations.

Several participants we interviewed noted that even though HFPP study results can help them identify suspect providers, they may still face challenges using the information to take corrective actions. HFPP participation rules require payers to examine their internal data and claims to investigate and build cases against suspect providers before taking any corrective actions, partly in order to minimize the risk of payers taking action on false positive study results. For certain types of fraud schemes, however, the participants' internal information alone may not provide enough evidence of improper billing. For instance, although an HFPP study may reveal clear evidence that a provider is billing multiple payers for an unreasonable number of services in a single day, the provider may have only billed individual payers for a limited, reasonable number of services.

Participants reported that HFPP has also facilitated both formal and informal information sharing among payers, and indicated that it has helped them learn about fraud vulnerabilities and strategies for effectively addressing them. Formal information sharing includes presentations at HFPP meetings and a whitepaper on how payers can help address beneficiary opioid abuse and reduce opioid-related fraud.[20] HFPP also manages a web portal where participants can share individual best practices and post "fraud alerts" about emerging fraud schemes or suspect providers. Informal information sharing includes knowledge exchanged through the networking and collaboration that occurs among HFPP participants, both at in-person HFPP meetings and through collaboration that occurs via the web portal's participant directory.

[20]See HFPP and NORC, *Healthcare Payer Strategies to Reduce the Harms of Opioids*, (January 2017), accessed February 6, 2017, https://downloads.cms.gov/files/hfpp/hfpp-opioid-white-paper.pdf.

HFPP Addressed Initial Data Sharing Concerns and Is Pursuing a New Data Sharing Strategy to Further Participants' Ability to Address Fraud

Although HFPP began operations in 2012, participants we interviewed stated that much of the initial work of the partnership involved negotiating the logistics for collecting and storing participants' claims data. CMS contracts with a trusted third party (TTP) entity to administer HFPP. The TTP consolidates, secures, and confidentially maintains the claims data shared by participants, and conducts studies that analyze the pooled data to identify potential fraud across payers. According to several participants we interviewed, some payers were initially reluctant to share claims data with the TTP because claims contain sensitive provider and beneficiary information and private payers may view them as proprietary. Accordingly, it took time for the TTP to demonstrate to payers its ability to securely store and use pooled claims data. Payers' reluctance resulted in an early time- and resource-intensive data sharing strategy that relied upon payers submitting a limited amount of claims data on a study-by-study basis, in a particular format, stripped of beneficiaries' personally identifiable information and protected health information.

Recently, HFPP began to pursue a new data sharing strategy. According to the TTP and participants we interviewed, payers will send in generalized data, reducing the data sharing burden on payers and enabling HFPP to conduct new types of studies to combat fraud. The data can be submitted in various formats, relieving payers from the need to extract and clean study-specific data. All participant data will be pooled and stored, and multiple studies will be run on the data submitted. Payers may voluntarily submit data that includes beneficiaries' personally identifiable information and protected health information. According to CMS officials, collection of personally identifiable information and protected health information will allow HFPP to conduct studies that involve identifying beneficiaries across payers, such as studies examining fraud schemes in which multiple providers fraudulently bill for the same beneficiaries.[21]

[21]CMS officials stated that beneficiary data will be de-identified by assigning beneficiaries HFPP-specific identification numbers. The de-identified beneficiary data will be stored for a period of time appropriate to conduct multiple studies.

Several HFPP participants we spoke with indicated their support of the new strategy and willingness to provide beneficiaries' personally identifiable information and protected health information for more in-depth HFPP studies. As of May 2017, 38 partners had signed data sharing agreements with the new TTP. However, not all payers that previously shared claims data have agreed to participate in the new data sharing strategy and those payers are still working with the TTP to formalize agreements regarding how their claims data will be stored and used.

Agency Comments

GAO provided a draft of this report to HHS. HHS provided technical comments, which GAO incorporated as appropriate.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we plan no further distribution until 30 days from the report date. At that time, we will send copies to the Secretary of Health and Human Services, the Administrator of CMS, appropriate congressional requesters, and other interested parties. In addition, the report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact me at (202) 512-7114 or at kingk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff that made key contributions to this report are listed in appendix I.

Kathleen M. King
Director, Health Care

List of Requesters

The Honorable Greg Walden
Chairman
The Honorable Frank Pallone
Ranking Member
Committee on Energy and Commerce
House of Representatives

The Honorable Kevin Brady
Chairman
Committee on Ways and Means
House of Representatives

The Honorable Michael C. Burgess
Chairman
The Honorable Gene Green
Ranking Member
Subcommittee on Health
Committee on Energy and Commerce
House of Representatives

The Honorable Tim Murphy
Chairman
The Honorable Diana DeGette
Ranking Member
Subcommittee on Oversight and Investigations
Committee on Energy and Commerce
House of Representatives

The Honorable Patrick J. Tiberi
Chairman
The Honorable Sander Levin
Ranking Member
Subcommittee on Health
Committee on Ways and Means
House of Representatives

The Honorable Vern Buchanan
Chairman
The Honorable John Lewis
Ranking Member
Subcommittee on Oversight
Committee on Ways and Means
House of Representatives

The Honorable Peter Roskam
House of Representatives

The Honorable Fred Upton
House of Representatives

Appendix I: GAO Contact and Staff Acknowledgments

GAO Contact

Kathleen M. King, (202) 512-7114, kingk@gao.gov

Staff Acknowledgments

In addition to the contact named above, Martin T. Gahart (Assistant Director), Michael Erhardt (Analyst-in-Charge), Muriel Brown, Cathleen Hamann, Colbie Holderness, and Jennifer Whitworth made key contributions to this report.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548