United States Government Accountability Office

GAO

Report to Congressional Requesters

October 2012

MEDICARE FRAUD PREVENTION

CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness

Accountability * Integrity * Reliability

GAO
Accountability * Integrity * Reliability
Highlights

Highlights of GAO-13-104, a report to congressional requesters

October 2012

MEDICARE FRAUD PREVENTION

CMS Has Implemented a Predictive Analytics System, but Needs to Define Measures to Determine Its Effectiveness

Why GAO Did This Study

GAO has designated Medicare as a high-risk program, in part because its complexity makes it particularly vulnerable to fraud. CMS, as the agency within the Department of Health and Human Services (HHS) responsible for administering Medicare and reducing fraud, uses a variety of systems that are intended to identity fraudulent payments. To enhance these efforts, the Small Business Jobs Act of 2010 provided funds for and required CMS to implement predictive analytics technologies—automated systems and tools that can help identify fraudulent claims before they are paid. In turn, CMS developed FPS.

GAO was asked to (1) determine the status of the implementation and use of FPS, (2) describe how the agency uses FPS to identify and investigate potentially fraudulent payments, (3) assess how the agency's use of FPS compares to private insurers' and Medicaid programs' practices, and (4) determine the extent to which CMS has defined and measured benefits and performance goals for the system. To do this, GAO reviewed program documentation, held discussions with state Medicaid officials and private insurers, and interviewed CMS officials and contractors.

What GAO Recommends

GAO recommends that CMS develop schedules for completing integration with existing systems, define and report to Congress quantifiable benefits and measurable performance targets and milestones, and conduct a post-implementation review of FPS. In its comments, HHS agreed with and described actions CMS was taking to address the recommendations.

View GAO-13-104. For more information, contact Valerie C. Melvin, (202) 512-6304, melvinv@gao.gov or Kathleen M. King at (202) 512-7114 or kingk@gao.gov.

What GAO Found

The Centers for Medicare and Medicaid Services (CMS) implemented its Fraud Prevention System (FPS) in July 2011, as required by the Small Business Jobs Act, and the system is being used by CMS and its program integrity contractors who conduct investigations of potentially fraudulent claims. Specifically, FPS analyzes Medicare claims data using models of fraudulent behavior, which results in automatic alerts on specific claims and providers, which are then prioritized for program integrity analysts to review and investigate as appropriate. However, while the system draws on a host of existing Medicare data sources and has been integrated with existing systems that process claims, it has not yet been integrated with the agency's payment-processing system to allow for the prevention of payments until suspect claims can be determined to be valid. Program officials stated that this functionality has been delayed due to the time required to develop system requirements; they estimated that it will be implemented by January 2013 but had not yet developed reliable schedules for completing this activity.

FPS is intended by program integrity officials to help facilitate the agency's shift from focusing on recovering large amounts of fraudulent payments after they have been made, to taking actions to prevent payments as soon as aberrant billing patterns are identified. Specifically, CMS has directed its program integrity contractors to prioritize alerts generated by the system and to focus on administrative actions—such as revocations of suspect providers' Medicare billing privileges—that can stop payment of fraudulent claims. To this end, the system has been incorporated into the contractors' existing investigative processes. CMS has also taken steps to address challenges contractors initially faced in using FPS, such as shifting priorities, workload challenges, and issues with system functionality.

Program integrity analysts' use of FPS has generally been consistent with key practices for using predictive analytics identified by private insurers and state Medicaid programs. These include using a variety of data sources; collaborating among system developers, investigative staff, and external stakeholders; and publicizing the use of predictive analytics to deter fraud.

CMS has not yet defined or measured quantifiable benefits, or established appropriate performance goals. To ensure that investments in information technology deliver value, agencies should forecast expected financial benefits and measure benefits accrued. In addition, the Office of Management and Budget requires agencies to define performance measures for systems that reflect program goals and to conduct post-implementation reviews to determine whether objectives are being met. However, CMS had not defined an approach for quantifying benefits or measuring the performance of FPS. Further, agency officials had not conducted a post-implementation review to determine whether FPS is effective in supporting efforts to prevent payment of fraudulent claims. Until program officials review the effectiveness of the system based on quantifiable benefits and measurable performance targets, they will not be able to determine the extent to which FPS is enhancing CMS's ability to accomplish the goals of its fraud prevention program.

Contents

Tables

Figures

Abbreviations

ASR	alert summary record
CMS	Centers for Medicare and Medicaid Services
CPI	Center for Program Integrity
FPS	Fraud Prevention System
HHS	Department of Health and Human Services
HIPAA	Health Information Portability and Accountability Act
MAC	Medicare Administrative Contractor
OIG	Office of Inspector General
OMB	Office of Management and Budget
One PI	One Program Integrity
PPACA	Patient Protection and Affordable Care Act
PSC	Program Safeguard Contractor
ZPIC	Zone Program Integrity Contractor

Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

October 15, 2012

The Honorable Thomas R. Carper
Chairman
The Honorable Scott Brown
Ranking Member
Subcommittee on Federal Financial Management, Government
Information, Federal Services, and International Security
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Tom Coburn, M.D.
United States Senate

Medicare is the federal program that helps pay for health care services for individuals aged 65 years and older, certain individuals with disabilities, and those with end-stage renal disease. In 2011, Medicare covered 48.4 million such eligible individuals with total program expenditures of $565 billion.[1]

For more than 20 years, we have designated Medicare as a high-risk program,[2] in part because its complexity makes it particularly vulnerable to fraud. Fraud involves an intentional act or representation to deceive with the knowledge that the action or representation could result in gain. We have previously reported that the deceptive nature of fraud makes its extent in the Medicare program difficult to measure in a reliable way, but it is clear that fraud contributes to Medicare's fiscal problems.[3]

The Centers for Medicare and 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. In this regard, CMS and its

[1] HHS, Fiscal Year 2011 Agency Financial Report (Washington, D.C.: Nov. 15, 2011).

[2] In 1990, we began to report on government operations that we identified as "high risk" for serious weaknesses in areas that involve substantial resources and provide critical services to the public. See GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

[3] GAO, *Medicare: Important Steps Have Been Taken, but More Could Be Done to Deter Fraud,* GAO-12-671T (Washington, D.C. April 2012).

contractors who help administer the program use various information technology systems to consolidate and analyze data to detect and investigate potentially fraudulent Medicare claims. To strengthen efforts toward preventing fraud in the program, the Small Business Jobs Act of 2010[4] provided funds for, and directed CMS to implement, predictive analytics technologies—a variety of automated systems and tools that can be used to identify particular types of behavior, including fraud, before transactions are completed. Toward this end, CMS developed its Fraud Prevention System (FPS) which, according to the agency, is intended to be used to analyze Medicare claims, provider, and beneficiary data before claims are paid to identify those that are potentially fraudulent. In doing so, CMS intends for FPS to support its efforts to move beyond the agency's traditional practice of detecting fraudulent claims and recovering funds after payment—an approach referred to as "pay and chase."

At your request, we conducted a study of CMS's Fraud Prevention System. Specifically, our objectives were to (1) determine the status of implementation and use of FPS within the agency's existing information technology infrastructure, (2) describe how the agency uses FPS to identify and investigate potentially fraudulent payments, (3) assess how the agency's use of FPS compares to private insurers' and Medicaid programs' practices, and (4) determine the extent to which CMS defined and measured benefits and performance goals for the system and has identified and met milestones for achieving those goals.

To determine the status of the implementation and use of FPS, we reviewed program management and planning documentation for the system. Specifically, to assess the extent to which FPS had been implemented, we compared the functionality implemented at the time of our study to requirements and plans defined in project management artifacts such as statements of work, work breakdown structures, and system release notes. To assess the extent to which FPS had been integrated within CMS's existing information technology infrastructure, we compared system documentation to agency modernization plans and other agency planning documents. To supplement this information, we discussed with agency officials their plans for and management of the FPS program's implementation efforts.

[4] Small Business Jobs Act of 2010, Pub.L.No. 111-240; § 4241, 124 Stat. 2504, 2599-2603 (Sept. 27, 2010) (codified at 42 U.S.C.§ 1320a-7m).

To describe how the agency uses FPS to identify and investigate potentially fraudulent payments, we interviewed CMS program integrity staff responsible for implementing FPS, observed demonstrations of the system, and reviewed relevant documents. These documents included the CMS Medicare Program Integrity Manual, CMS guidance and directions to the contractors related to FPS, and educational materials for using FPS. We conducted site visits to and interviewed officials by phone from the Medicare contractors responsible for fraud investigations in specific geographical zones.

To assess how the agency's use of FPS compares to private insurers' and Medicaid programs' practices, we examined the use of similar systems by private health insurers and Medicaid programs and compared observations from their experiences to CMS's current and planned practices for conducting predictive analysis. Our observations are based on interviews with five state Medicaid agencies and nine private insurance companies that we identified as having knowledge about predictive data analytics.

To determine the extent to which CMS defined and measured benefits and performance goals for the system and identified and met milestones for achieving those goals, we discussed efforts to define benefits and performance measures with relevant agency officials and compared the outcomes of their efforts to information technology program reporting requirements established by the Office of Management and Budget (OMB). To determine the agency's progress toward achieving goals and objectives for improving program integrity outcomes through the use of FPS, we reviewed the agency's strategic plan and program planning documents to identify program-level goals, and assessed the extent to which the system's performance plans and objectives supported efforts to achieve program goals. We also examined reports submitted by CMS to OMB that included information about the system's expected performance, and interviewed program officials about steps the agency had taken to achieve the goals and objectives. A more detailed discussion of our objectives, scope, and methodology is included in appendix I.

We conducted this performance audit from October 2011 to October 2012 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

The fee-for-service part of the Medicare program processes more than a billion claims each year from about 1.5 million providers of health care or related services and equipment to beneficiaries. These providers bill Medicare for their services and supplies which, among other things, consist of inpatient and outpatient hospital services, physician services, home health care, and durable medical equipment (such as walkers and wheelchairs). Preventing fraud and ensuring that payments for these services and supplies are accurate can be complicated, especially since fraud can be difficult to detect, as those involved are engaged in intentional deception. For example, fraud may involve providers submitting claims with false documentation for services not provided, which may appear to be valid.

To address Medicare's vulnerability to fraud, Congress enacted a provision in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) that established the Medicare Integrity Program.[5] HIPAA provides this program with dedicated funds to identify and combat improper payments, including those caused by fraud. In addition, when Congress passed the Patient Protection and Affordable Care Act (PPACA) in 2010,[6] it provided CMS with additional authority to combat Medicare fraud, and set a number of new requirements specific to the program. For example, PPACA gave CMS the authority to suspend payment of Medicare claims pending an investigation of a credible allegation of fraud and required it to conduct certain new provider and supplier enrollment screening procedures intended to strengthen the process, such as checking providers' licensure.

The Center for Program Integrity and Program Integrity Contractors

In April 2010, CMS established the Center for Program Integrity (CPI) to enable a strategic and coordinated approach to program integrity initiatives throughout the agency and to build on and strengthen existing program integrity efforts.[7] As the component responsible for overseeing

[5] Pub. L. No. 104-191, § 202, 110 Stat. 1996-98 (codified at 42 U.S.C. § 1395ddd).

[6] Pub. L. No. 111-148, 124 Stat.119 (2010), as amended by the Health Care and Education Reconciliation Act of 2010, Pub. L. No. 111-152, 124 Stat. 1029, which we refer to collectively as PPACA.

[7] CPI was created as part of a CMS restructuring. In addition to Medicare, CPI is responsible for ensuring program integrity for Medicaid and Children's Health Insurance Program. See 75 Fed. Reg. 14176 (Mar. 24, 2010).

the agency's Medicare program integrity efforts, the center's mission is to ensure that correct payments are made to legitimate providers for covered, appropriate, and reasonable services for eligible beneficiaries.

To accomplish its mission, the center has undertaken a strategy to supplement the agency's "pay and chase" approach, which focuses on the recovery of funds lost due to payments of fraudulent claims, with an approach that is directed toward the detection and prevention of fraud before claims are paid. The strategy has concurrent objectives to (1) enhance efforts to screen providers and suppliers enrolling in Medicare to prevent enrollment by entities that might attempt to defraud or abuse the Medicare program and (2) detect aberrant, improper, or potentially fraudulent billing patterns and take quick actions against providers suspected of fraud. In addressing the second objective, CPI intends to use predictive analytics technologies to detect potential fraud and prevent payments of claims that are based on fraudulent activities. Accordingly, CPI is the focal point for all activities related to FPS.

CPI uses contractor services to support the agency's program integrity initiatives. Among these are contractors tasked with specific responsibilities for ensuring that payments are not made for claims that are filed incorrectly or that are identified as being associated with potentially fraudulent, wasteful, or abusive billing practices. Specifically, Medicare Administrative Contractors (MAC)[8] are responsible for processing and paying Medicare fee-for-service claims, and Zone Program Integrity Contractors (ZPIC) are responsible for identifying and investigating potential fraud in the program.[9]

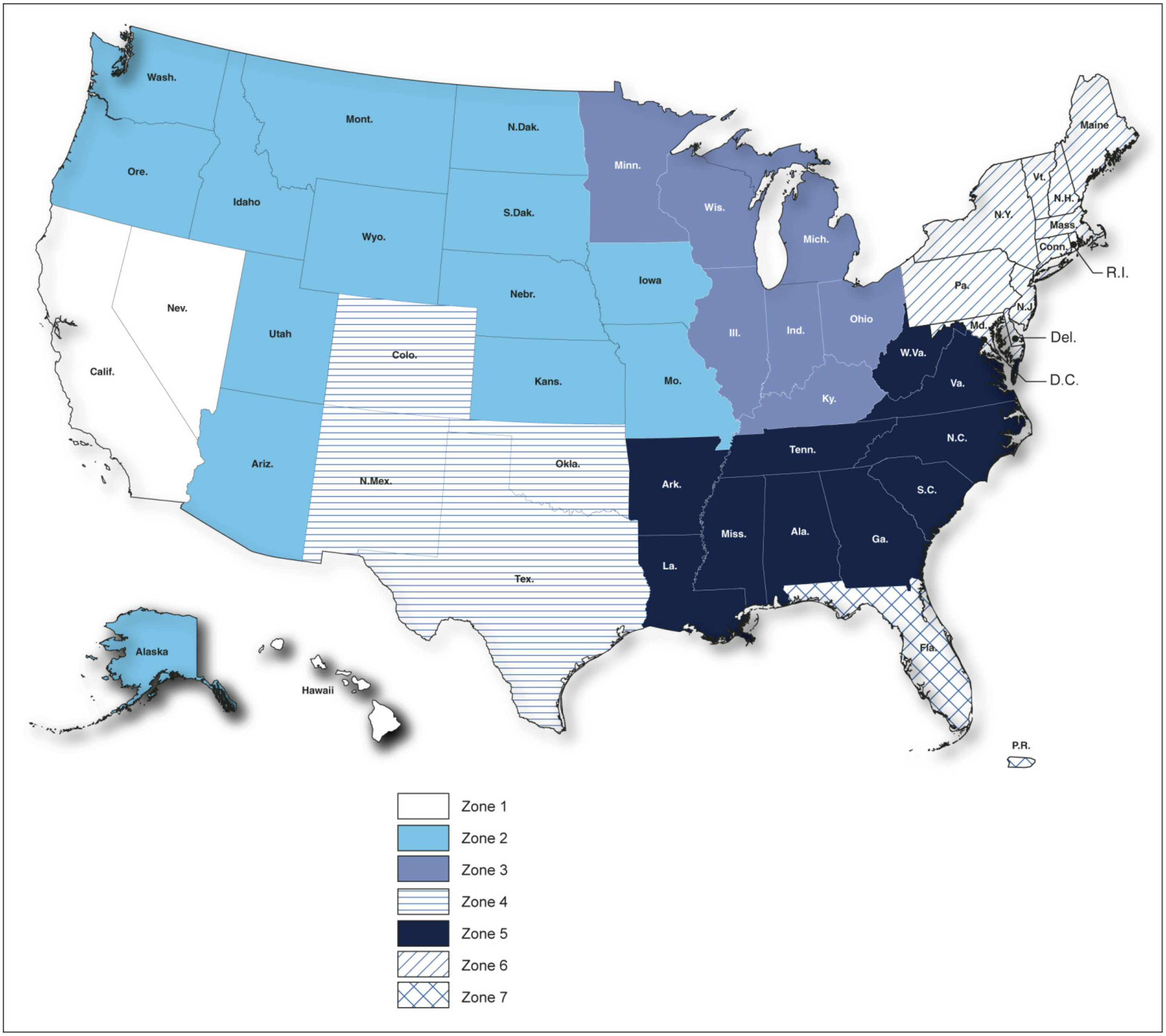
[8] In response to contracting reform requirements in the Medicare Prescription Drug, Improvement, and Modernization Act of 2003, CMS has been transitioning its claims processing contracts to MACs. While CMS has not yet fully transitioned claims processing responsibilities from its legacy contractors to the MACs, we use the term MACs to refer to all claims administration contractors.

[9] CMS is in the process of replacing its legacy Program Safeguard Contractors (PSC) with the seven ZPICs. The PSCs were responsible for program integrity for specific parts of Medicare, such as Part A, whereas the ZPICs are responsible for program integrity for both Parts A and B, or fee-for-service, within their geographic zones. As of April 2012, all but one ZPIC had been implemented. The existing PSCs are continuing to conduct work for that zone until the contract for the relevant ZPIC is finalized. We refer to program integrity contractors as ZPICs throughout the report.

When processing claims, MACs review them prior to payment to ensure that payments are made to legitimate providers for reasonable and medically necessary services covered by Medicare for eligible individuals. The systems that the MACs use for processing and paying claims, called “shared systems,” execute automated prepayment controls called “edits,” which are instructions programmed into the system software to identify errors in individual claims and prevent payment of incomplete or incorrect claims. For example, prepayment edits may identify claims for services unlikely to be provided in the normal course of medical care, such as more than one appendectomy on the same beneficiary and other services that are anatomically impossible. Most of the prepayment edits implemented by CMS and its contractors are automated, meaning that if a claim does not meet the criteria of the edit, payment of that claim is automatically denied. However, while these prepayment edits are designed to prevent payment errors that can be identified by screening individual claims, they cannot detect providers’ billing or beneficiaries’ utilization patterns that may indicate fraud. Specifically, the capability to collect and analyze data that are submitted over a period of time is necessary for a system to be able to identify patterns in behavior.

ZPICs are responsible for identifying and investigating potential fraud in the Medicare fee-for-service program. CPI directs and monitors their activities. These contractors identify claims and provider billing patterns that may indicate fraud and investigate leads from a variety of sources, including complaints and tips lodged by beneficiaries. ZPICs operate in seven geographical zones across the country, and each ZPIC is responsible for conducting program integrity activities in its geographic jurisdiction. (Fig. 1 depicts the ZPIC zones and corresponding geographic areas.) Varying levels of fraud risk prevail across the zones. For example, Zone 7 includes an area known to be at high risk of fraud, while Zone 2 covers a geographically large and predominantly rural area that may be at a lower risk of fraud.

Figure 1: ZPIC Zones and Geographic Areas



Source: GAO analysis of agency data; MapArt (map).

Note: As of April 2012, the ZPIC contract for Zone 6 had yet to be implemented, and legacy PSCs were still operating in that zone.

The ZPICs include about 510 data analysts, investigators, and medical record reviewers.[10] Data analysts use automated tools to analyze data on claims, providers, and beneficiaries in their efforts to identify fraud, support investigations, and search for new fraud schemes. Investigators examine fraud leads by performing a range of investigative actions, such as provider reviews and interviews with beneficiaries and providers. The medical record reviewers examine medical records and provide clinical knowledge needed to support analysts' and investigators' work.

As a result of their analyses and investigations, ZPICs may refer to law enforcement and initiate administration actions against providers suspected of fraud. Specifically, if the contractors uncover suspected cases of fraud, they refer the investigation to the HHS Office of Inspector General (OIG) for further examination and possible criminal or civil prosecution. ZPICs also initiate a range of administrative actions, including revocations of providers' billing privileges and payment suspensions, which allow CMS to stop payment on suspect claims and prevent the payment of future claims until an investigation is resolved.[11] They initiate administrative actions by recommending the actions to CMS and coordinating with the MACs to carry them out. For example, ZPICs recommend payment suspensions to CMS and, if CMS approves, the MACs implement the suspension. Table 1 describes the types of administrative actions ZPICs can recommend against providers.

[10] This approximation of the number of ZPIC staff represents zones 1, 2, 4, 5, and 7, which were fully operational in early April 2012. It does not include the legacy PSCs that were operating in Zone 6, nor does it include ZPIC staff in Zone 3 which did not become fully operational until the end of April 2012.

[11] While CMS had the authority to impose payment suspensions prior to PPACA, the law specifically authorized CMS to suspend payments to providers pending the investigation of credible allegations of fraud. CMS is required to consult with the HHS OIG in determining whether a credible allegation of fraud exists.

Table 1: Administrative Actions Taken by ZPICs

Action	Definition
Implementation of prepayment review edits	Provider-specific prepayment edits are used to identify claims for medical review.[a]
Implementation of beneficiary- or provider-specific edits	Beneficiary- or provider-specific prepayment edits are used to prevent payment for non-covered, incorrectly coded, or inappropriately billed services.[a]
Revocation	A provider's Medicare billing privileges are terminated.
Payment suspension	Medicare payments to a provider are suspended, in whole or in part.
Overpayment determination	Medicare payments received by a provider are in excess of amounts due and payable.

Source: CMS.

[a] In cases of suspected fraud, ZPICs can recommend the implementation of prepayment edits that apply to specific providers and automatically deny claims or flag claims for prepayment review. In these cases, prepayment edits are considered by CMS to be administrative actions.

CMS and Its Contractors Have Used Information Technology to Detect Payments of Fraudulent Claims

CMS and its contractors have, for more than a decade, used information technology systems to support efforts to identify potential fraud in the Medicare program. These systems were developed and implemented to analyze claims data in support of program integrity analysts' efforts to detect potentially fraudulent claims after they were paid so that actions could be taken by CMS to collect funds for the payments made in error (i.e., the pay-and-chase approach). For example, in 2002 CMS implemented its Next Generation Desktop to provide data regarding beneficiaries' enrollment, claims, health care options, preventive services, and prescription drug benefits. This system is also used as an analytical tool during investigations and provides enhanced data to law enforcement personnel, such as data about complaints against providers reported by beneficiaries. Further, in 2006, CMS implemented the One Program Integrity (One PI) system for use in helping to identify claims that were potentially fraudulent and to recover the funds lost because of payments made for claims determined to be fraudulent. The system was intended to enable CMS's program integrity analysts and ZPICs to access from a centralized source the provider and beneficiary data related to claims after they have been paid. As a result of our prior study of One PI, in June 2011 we made a series of recommendations regarding the status of the implementation and use of the system.[12] In commenting on the results of our study, agency officials agreed with all of them, including recommendations that CMS define measurable financial benefits expected from the implementation of the system and establish outcome-based performance measures that gauge progress toward meeting program goals that could be attributed to One PI.

In addition to systems and tools provided and maintained by CMS, the ZPICs have developed and implemented their own information technology solutions to analyze claims and provider data in their efforts to detect potentially fraudulent claims that were paid by Medicare. For example, the ZPICs have their own case management systems and custom-developed algorithms for analyzing data from their zone-specific databases that can supplement the data and tools available from CMS. The ZPICs can also incorporate data from other sources into their databases, including data from state databases on provider licensing and incorporated businesses, and Internet searches of research websites.

While the program integrity contractors have been using these systems to support CMS's efforts to identify improper and potentially fraudulent payments of Medicare claims, they have not previously had access to information technology systems and tools from CMS that were designed specifically to identify potentially fraudulent claims before they were paid. In this regard, CMS intends to use predictive analytics as an innovative component of its fraud prevention program.

CMS Developed FPS to Help Prevent Payment of Potentially Fraudulent Claims

To advance the use of predictive analytics technologies to help prevent fraud in the Medicare program, the Small Business Jobs Act of 2010 appropriated $100 million to CMS, to remain available until expended, for the development and implementation of a predictive analytics system. Enacted on September 27, 2010, the law required CMS to implement a system that could analyze provider billing and beneficiary utilization patterns in the Medicare fee-for-service program to identify potentially fraudulent claims before they were paid. To do this, the system was to capture data on Medicare provider and beneficiary activities needed to

[12] GAO*, Fraud Detection Systems: Centers for Medicare and Medicaid Services Needs to Ensure More Widespread Use,* GAO-11-475 (Washington, D.C.: June 30, 2011), and *Fraud Detection Systems: Additional Actions Needed to Support Program Integrity Efforts at CMS,* GAO-11-822T (Washington, D.C.: July 12, 2011).

provide a comprehensive view across all providers, beneficiaries, and geographies. It was also intended to identify and analyze Medicare provider networks, provider billing patterns, and beneficiary utilization patterns to identify and detect suspicious patterns or anomalies that represent a high risk of fraudulent activity. The act further required the system to be integrated into Medicare's existing systems and processes for analyzing and paying fee-for-service claims in order to prevent the payment of claims identified as high risk until such claims were verified to be valid.

The act also specified when and how CMS should develop and implement the system. Specifically, it required that CMS select at least two contractors to complete the work and that the system be developed and implemented by July 1, 2011, in the 10 states identified by CMS as having the highest risk of fraud. The act further required the Secretary of HHS to issue, no later than September 30, 2012, the first of three annual implementation reports that identify savings attributable to the use of predictive analytics, along with recommendations regarding the expanded use of predictive analytics to other CMS programs.[13] The act stated that based on the results and recommendations of the first report, the use of the system was to be expanded to an additional 10 states at the next highest risk of fraud on October 1, 2012; similarly, based on the second report, the use would then be expanded to the remaining states, territories, and commonwealth on January 1, 2014.

To meet the act's requirements, CMS assigned officials within CPI responsibility for the development, implementation, and maintenance of FPS. These officials included a business process owner, information technology program manager, information technology specialist, and contracting officer. In defining requirements for the system to address the mandate of the Small Business Jobs Act, these program officials planned to implement by July 1, 2011, system software for analyzing fee-for-service claims data, along with predictive analytic models that use historic Medicare claims and other data to identify high-risk claims and providers.

[13] The reports are to include a certification by the HHS OIG that specifies the actual and projected savings to Medicare fee-for-service from the use of predictive analytics, including estimates of the amounts of improper payments recovered and avoided, along with actual and projected savings and return on investment of each predictive analytics technology implemented. Further, by September 2015, CMS is required to report on the cost-effectiveness of its use of predictive analytics and the potential for expanding its use to Medicaid and the Children's Health Insurance Program.

Program officials further planned, by July 2012, to implement functionality into FPS to enable automatic notification to system users of potentially fraudulent claims and to prevent payments of those claims until program integrity analysts determined that they were valid.

In April 2011, CMS awarded almost $77 million to a development contractor to implement, operate, and maintain the system software and to design a first set of models for the initial implementation of FPS.[14] The agency awarded about $13 million to a second contractor in July 2011 to develop additional models that could be integrated into the system.[15] CPI also engaged its internal program integrity analysts to help design the models and test the initial implementation of the system.

FPS is a web-based system that is operated from a contractor's data center and accessed by users via the agency's secured private network. The system is comprised of software that analyzes fee-for-service claims data as the claims are being processed for payment, along with hardware, such as servers that support connections between users' facilities and CMS's network, and devices that store the data used and generated by the system. The system software and predictive models are designed to analyze the claims data and generate alerts to users when the results of analyses identify billing patterns or provider and beneficiary behavior that may be fraudulent and warrant administrative actions.

In September 2011, CPI established a group that works with and provides training to the ZPICs on how to use FPS to initiate administrative actions more quickly against providers suspected of fraud. According to CPI officials, they intend to continue to refine the system to provide analysts

[14] CMS officials described the system software as an "off-the-shelf" product that had been in use by a large telecommunications company for about 10 years. While the system software and predictive models were used by that company to help detect potentially fraudulent transactions, they were not used for health-care-related purposes. The models to be used with CMS's implementation of the software are developed specifically for CMS's fraud prevention purposes.

[15] The development contract was awarded to Northrop Grumman Information Technology, Inc.; the modeling contract was awarded to International Business Machines (IBM) Corporation. The total contract amount, about $90 million, was awarded for a performance period of 4 years and is subject to annual renewals based on performance appraisals. According to program officials, the amount committed for the first year of the contractors' work was $30.5 million.

and investigators with data and statistical information useful in conducting investigations based on input provided during these training sessions.

FPS Has Been Implemented and Is in Use, but It Is Not Yet Fully Integrated with CMS's Existing Information Technology Systems

In response to the Small Business Jobs Act, CMS implemented its initial release of FPS by July 1, 2011. While the act called for CMS to first implement the system for use in the 10 states identified by CMS as having the highest risk of fraud, the agency chose to deploy the system to all the ZPIC geographic zones. In addition, the system was integrated with existing data sources and systems that process claims, but it was not yet integrated with CMS's claims payment systems. As of May 2012, CMS had spent nearly $26 million on the implementation of FPS. Of this amount, about $1 million was spent for internal CMS staff and $25 million for the development and modeling contractors.

CMS's initial release of the system consisted of system software for analyzing fee-for-service claims data and predictive analytic models that use historic Medicare claims and other data to identify high-risk claims and providers. After the initial release, CMS implemented three more releases of software through July 1, 2012, that incorporated changes or enhancements to the system as well as additional models. The four system releases yielded a total of 25 predictive analytic models in three different categories and with varying levels of complexity. Specifically, these consisted of the following model types:

- Rules-based models, which are to filter potentially fraudulent claims and behaviors, such as providers submitting claims for an unreasonable number of services. These models also are intended to target fraud associated with specific services, including those that CMS has stated are at high risk for fraud, such as home health agency services and durable medical equipment suppliers.[16] These are the simplest types of models since the analysis conducted using them only involves counting or identifying types of claims and comparing the results to established thresholds.

- Anomaly-detection models, which are to identify abnormal provider patterns relative to the patterns of peers, such as a pattern of filing claims for an unreasonable number of services. These models generate analyses that are more complex because they require

[16] GAO-12-671T.

identification of patterns of behavior based on data collected over a period of time, and comparisons of those patterns to established behaviors that have been determined to be reasonable.

- Predictive models, which are to use historical data to identify patterns associated with fraud, and then use these data to identify certain potentially fraudulent behaviors when applied to current claims data. These models are intended to help identify providers with billing patterns associated with known forms of fraud. This is the most complex type of model implemented into FPS because it not only requires analysis of large amounts of data but may also require detection of several patterns of behavior that individually may not be suspicious but, when conducted together, can indicate fraudulent activity.

Of the 25 models that CMS had implemented by July 1, 2012, 14 were rules-based, 8 were anomaly-detection, and 3 were predictive. Table 2 describes the four releases of FPS, including the numbers and types of models.

Table 2: Status of FPS Releases, Models, and Time Frames as of July 1, 2012

Release	Description	Release date	Number of new models
1.0	Implementation of initial predictive analytics system and models	6/30/2011	8 (5 rules-based and 3 anomaly-detection)
2.0	Implementation of new models and system enhancements	12/16/2011	6 (4 rules-based and 2 anomaly-detection)
3.0	Implementation of new models and system enhancements	4/16/12	5 (3 rules-based and 2 predictive)
4.0	Implementation of new models and system enhancements	6/25/12	6 (2 rules-based, 3 anomaly-detection, and 1 predictive)
Total			**25[a] (14 rules-based, 8 anomaly-detection, and 3 predictive)**

Source: GAO analysis of CMS data.

[a] FPS officials stated that after counting discontinued and multiple versions of models, which they considered to be significantly enhanced or improved versions of pre-existing models, they had implemented 37 models (including 3 models that were discontinued because they generated too many false positives and 9 additional versions applied to 6 different models). However, 25 different models were operational with release 4.0.

While the act called for first implementing the system in the 10 states at highest risk of fraud and incrementally assessing and expanding its use throughout the country until January 2014, program officials stated that analysts in all the zones—and covering all states—were provided the ability to access and use FPS when it was initially implemented. The officials stated that they took this approach because program integrity activities are implemented and managed within the seven zones rather than by states, and the 10 highest-risk states were dispersed across multiple ZPIC zones. According to the officials, making the system available to the 10 highest-risk states thus required making it accessible to all of the zones. Program officials further stated that use of the system by ZPICS in all the zones was intended to provide a national view of claims data and to allow the identification and tracking of fraud schemes that crossed zones.

The FPS business owner added that while analysts assigned to the ZPICs were the primary intended users of FPS, the system was also made available to CMS's internal program integrity analysts and to investigators with HHS OIG. System reports showed that during the first year of implementation, CMS authorized almost 470 analysts and investigators from the ZPICs, CMS, and the HHS OIG to use FPS, including about 80 from legacy Program Safeguard Contractors (PSC). Program officials reported that, of these, almost 400 analysts were actively using the system as of April 2012. Moreover, program officials told us that the system was being used by almost all the program integrity analysts expected to do so.

To use the system, program integrity analysts access FPS via CMS's secured network from workstations within their facilities. As noted during our observation of a demonstration at CMS's offices, FPS processed and analyzed claims data using the models, then prioritized the claims data for review based on whether they were consistent with scenarios depicted by the models. When the system identified high-risk claims data, it generated an alert based on that data. As more claims were screened throughout the day, the system automatically continued to generate alerts associated with individual providers. It then generated alert summary records (ASRs) for the providers and scored the risk level of the records based on collective results of the individual alerts. The system notified FPS users of the ASRs. The analysts using the system were to review the ASRs and conduct additional research to determine whether further investigation was needed to verify that the related claims were valid.

As required by the act, CMS integrated FPS with existing data sources and systems that process claims. To integrate FPS with CMS's existing information technology infrastructure, the contractors tasked to develop the system and models were required to capture data from several existing sources needed to provide a comprehensive view of activities across providers, beneficiaries, and geographies. Access to these sources was also needed to allow for analysis of Medicare provider networks, along with billing and beneficiary utilization patterns, in order to identify suspicious patterns or anomalies that could indicate fraud. For example, these data provide information about historical activities, including any suspicious activities related to a particular service or provider that had been noted in the past, or about the status of providers' enrollment in the Medicare fee-for-service program. Thus, the data are needed by FPS to analyze incoming claims data to identify patterns of behavior like those known to indicate fraud. According to program officials and our review of system specifications, the contractors integrated supporting data from various sources, as identified in table 3.

Table 3: FPS Data Sources

Source	Description
Common Working File	Contains Medicare beneficiary eligibility information. Claims are transmitted to the Common Working File during processing to determine a beneficiary's eligibility, among other things. This system provides Part A and B data (excluding durable medical equipment) for claims that have already been processed by the MACs.
Common Electronic Data Interchange	Provides claims data for durable medical equipment claims that have not yet been processed by the MACs.
National Fraud Investigation Database	Contains data related to Medicare fraud and abuse investigations, cases, and payment suspensions by ZPICs. These data are used to provide a tag, or indicator, in FPS that an alert is associated with a case in this database.
Compromised Number Database	Contains data on beneficiary and provider identification numbers that have been compromised–i.e., stolen or used without a provider's or beneficiary's knowledge.
Next Generation Desktop	Contains data on complaints provided to CMS by beneficiaries. Data are used to provide a tag, or indicator, to FPS that the provider who is the subject of an alert has also had recent complaints made against them.
Provider Enrollment Chain and Ownership System	Provides information on providers and suppliers enrolled in the Medicare program, such as identifiers and addresses, to use during claims analysis.
Integrated Data Repository	Contains various Part A, B, C, and D entitlement, enrollment, and utilization data. These data are used to develop tables in FPS that include history information needed by models for claims analysis.

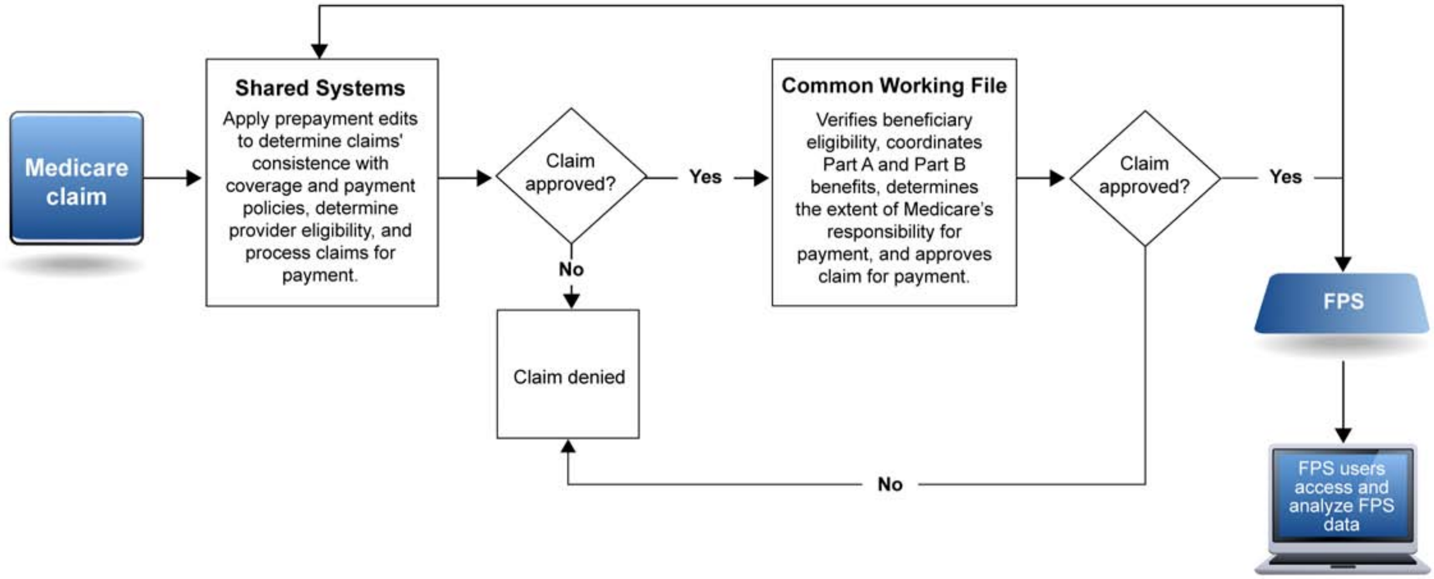
Source: GAO analysis of CMS data.

To facilitate analyses of claims data, fee-for-service and durable medical equipment claims are first transmitted to FPS from CMS's Common Working File and the Common Electronic Data Interchange (both described in table 3). The system analyzes the claims data based on the types of models integrated into the system and the supporting data extracted from other CMS data sources, such as the Integrated Data Repository and the Provider Enrollment Chain and Ownership System.

FPS's analytical capabilities were integrated with CMS's existing systems for processing fee-for-service claims, as required by the act. In describing this integration, program officials stated that claims data for medical services are transmitted to FPS after prepayment edits are applied by the "shared systems" (systems that the MACs use to process claims)--usually 3 to 5 days from the time claims are submitted to CMS. All the fee-for-service claims data are transmitted to FPS at the same time they are submitted to the payment processing component of the shared systems.[17] Figure 2 illustrates the integration of FPS claims analysis with CMS's existing fee-for-service claims processing systems.

[17] According to FPS officials, claims for payment of durable medical equipment are obtained by FPS from different systems and as a result they are not subject to the shared systems prepayment edits.

Figure 2: Data Flow of Fee-for-Service Claims through CMS's Systems for Processing and Paying Claims


Medicare claim
Shared Systems
Apply prepayment edits to determine claims' consistence with coverage and payment policies, determine provider eligibility, and process claims for payment.
Claim approved?
Yes
No
Claim denied
Common Working File
Verifies beneficiary eligibility, coordinates Part A and Part B benefits, determines the extent of Medicare's responsibility for payment, and approves claim for payment.
Claim approved?
Yes
No
FPS
FPS users access and analyze FPS data

Source: GAO analysis of CMS data.

While FPS was integrated with existing data sources and systems that process claims, it had not been further integrated with CMS's claims payment systems. Specifically, FPS had not been integrated with the components of the shared systems that process the payment of claims. However, this level of integration is required to enable FPS to prevent the payment of potentially fraudulent claims until they have been verified by program integrity analysts and investigators.

While the act called for the implementation of FPS by July 1, 2011, including this capability, the agency's program plans initially indicated that it was to be implemented by July 1, 2012. However, the business process owner of FPS stated that planning for the development of this system functionality required extensive discussions regarding design and requirements with entities that maintain and use other systems, particularly the shared systems. Consequently, FPS program officials did not complete requirements definition until May 2012. The official told us, and high-level program plans and schedules indicate, that CMS now intends to complete integration of the capability in January 2013.

Although CMS has identified January 2013 as a target date for completing the development, testing, and integration of FPS with the claims payment systems, program officials had not yet defined detailed schedules for completing the associated tasks required to carry this out. Best practices, such as those described in our cost estimation guide,[18] emphasize the importance of establishing reliable program schedules that include all activities to be performed; assign resources (labor, materials, etc.) to those activities; identify risks and their probability; and build appropriate reserve time into the schedule. However, FPS program officials had not yet developed such schedules and did not indicate when they intend to do so. Until it develops reliable schedules for completing associated tasks, the agency will be at risk of experiencing additional delays in further integrating FPS with the payment processing system, and CMS and its program integrity analysts may lack the capability needed to prevent payment of potentially fraudulent claims identified by FPS until they are determined by program integrity analysts to be valid.

CMS Is Using FPS to Identify and Investigate Potential Fraud

While CMS has not integrated FPS with its claims-payment system, it is using FPS to change how potential fraud is identified and investigated as part of its fraud prevention strategy. CMS has directed the ZPICs to incorporate the use of FPS into their processes and investigate high-risk leads generated by the system. The contractors with whom we spoke stated that investigations based on leads generated by FPS are similar to those from other sources. Further, CMS has taken steps to address certain initial challenges that ZPICs encountered in using FPS.

CMS Is Using FPS to Change How Potential Fraud Is Identified and Investigated as Part of Its Fraud Prevention Strategy

CMS is using FPS to identify providers with aberrant billing patterns and prioritize those providers for investigation as part of its strategy to prevent Medicare fraud. With the implementation of the system, CMS directed the ZPICs to prioritize investigations of leads from the system that meet certain high-risk thresholds. CMS program integrity officials stated that, as of April 2012, about 10 percent of ZPIC investigations were initiated as a result of using FPS. By prioritizing these investigations, these officials told us that they intend for ZPICs to target suspect providers for investigation as soon as aberrant billing patterns that are consistent with fraud are identified, rather than targeting providers that have already received large amounts of potentially fraudulent payments. In addition, investigations of leads from FPS should be faster because the leads provide information

[18] GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009).

about the type of fraud being identified, and the system is designed to provide investigators with data and statistical tools to conduct investigations. CMS program integrity officials also told us that the agency intends to use FPS to deny only a small number of claims without further investigation once it completes integration of FPS with its claims-payment system and that ZPICs will continue to coordinate with the MACs to take administrative actions against providers.

In addition to directing ZPICs to investigate leads from FPS, CPI also established a working group, referred to as the command center, to work with and provide training to the ZPICs on how to use the system to initiate administrative actions more quickly against providers suspected of fraud. On a recurring basis, typically every 2 weeks, select staff from a ZPIC travel to CMS to receive training related to the system and to discuss current FPS trends and investigations. CMS officials stated that these training sessions and discussions help the analysts develop new and streamlined approaches for gathering evidence and taking action against providers suspected of potential fraud. For example, CMS conducted training with ZPIC staff on how to investigate system leads that target certain forms of fraud, such as fraud associated with home health services. In addition, ZPICs received training on how best to use the system to ensure that resulting administrative actions, such as revocations of providers' billing privileges, are well supported by the evidence. For example, ZPICs received training on Medicare revocation policies and processes and were provided with examples of successful revocations that were initiated based on system leads. Finally, based on these training sessions, CMS continues to refine the system to provide investigators with data and statistical information useful in conducting investigations.

Concurrent with the implementation of FPS and to further help move away from its pay-and-chase approach to detecting fraud, CMS has directed the ZPICs to focus on recommending and initiating administrative actions—especially the revocation of Medicare billing privileges—against providers suspected of fraud. As directed by CMS, ZPICs previously focused their investigative efforts on gathering evidence to verify overpayments and developing criminal and civil cases for law enforcement agencies—a lengthy process that often involved many investigative steps. In particular, CMS program integrity and ZPIC officials cited the large amount of time and resources involved in reviewing medical records—an investigative process in which staff with clinical backgrounds review claims to determine whether billed services are potentially fraudulent or inconsistent with clinical practice. According to

CMS program integrity officials, the information provided by FPS is well-matched with the evidence necessary for ZPICs to recommend revocations against providers without having to conduct extensive investigations. These officials also told us that they have directed the ZPICs to focus on pursuing revocations because revocations prohibit providers suspected of fraud from billing Medicare. Moreover, revoking a provider's enrollment limits the need to expend additional resources tracking their claims or gathering evidence to justify the denial of suspect claims as compared to other administrative actions, such as suspension of payments to suspect providers.

ZPICs Have Incorporated FPS into Their Processes and Report That Investigations of FPS Leads Are Similar to Other Investigations

All of the ZPICs have integrated FPS into their existing processes for identifying and investigating potentially fraudulent claims and providers. All but one of the ZPICs established FPS teams as a way to incorporate the system into their processes. These teams consist of ZPIC staff designated as the primary users of the system. The ZPICs generally take the following steps when using FPS:

- *Monitor FPS and triage its investigative leads:* Since CMS requires the ZPICs to conduct preliminary reviews of high-risk leads from the system, staff on the FPS teams monitor the system for new investigative leads—ASRs—that exceed the high-risk thresholds. CMS requires the ZPICs to determine whether the providers associated with those leads are "suspect" or "non-suspect." These reviews are often conducted by the FPS teams. ZPIC officials told us that they often look for certain patterns associated with fraud when making this determination. For instance, identification of a provider that bills for a small number of beneficiaries but an excessive number of services may lead to a suspect determination.

- *Refer suspect providers for further investigation:* Suspect leads become formal investigations of the provider and are generally referred to other ZPIC investigators for further investigation. For example, a lead from FPS related to home health services may be referred to an investigator with expertise in that area.

- *Conduct investigation:* Once a lead from the system is assigned to an investigator, it is investigated similarly to other leads. The investigator can take multiple investigative actions to determine whether the provider is engaged in potential fraud including interviewing the provider and the provider's beneficiaries, conducting onsite audits to review a provider's records and assess whether the provider's facilities are appropriate for the services provided, determining whether there are other complaints against the provider, and conducting additional data analysis using FPS and other tools. The ZPICs can refer suspect providers to HHS OIG or recommend them for administrative actions.

Officials from the ZPICs reported that FPS has not fundamentally changed the way in which they investigate fraud. The system has not, according to ZPIC officials, significantly sped up investigations or enabled quicker administrative actions in most instances. Instead, officials reported that leads from the system were broad indicators that particular providers were suspect, but did not in all cases provide sufficient evidence of potentially fraudulent billing to allow for faster investigations or resolutions. FPS investigations were similar to those from other sources in that they often required additional investigative steps, such as beneficiary and provider interviews.

On the other hand, ZPICs reported certain advantages as a result of using FPS. For example, analysts can query the system for specific data to support their analysis of leads and export data from FPS into other systems they use to conduct additional analysis of claim lines flagged by FPS. Data generated by the system may also notify investigators of information available in other CMS databases, such as the national Fraud Investigation Database. In addition, using FPS's near-real-time claims data, some investigators reported identifying and conducting interviews with beneficiaries shortly after they received services from providers under investigation, when beneficiaries can better recall details about their care. Finally, information in FPS has also helped substantiate leads from other sources. For example, one ZPIC noted that its investigators use information from the system to help verify tips and complaints about suspected fraud.

CMS Has Taken Steps to Address Initial Challenges ZPICs Had Using FPS

All ZPICs that we interviewed told us that they experienced initial challenges using FPS. CMS has been responsive to many of these challenges and has developed processes for soliciting and incorporating ZPIC input and feedback on the system and its use. Certain ZPICs attributed some early challenges with the system to CMS not soliciting their input during the development and initial implementation of FPS. CMS has since developed a process in which ZPICs submit “change requests” to propose changes to the system’s functionality and enhancements to the models so that they better target suspect providers. The command center also serves as a forum for ZPICs to discuss and provide feedback on FPS and its use. These processes for soliciting and implementing feedback are consistent with key practices we have previously identified for implementing management initiatives.[19] In particular, feedback can provide important insights about operations from a front-line perspective.

The challenges ZPICs faced using FPS centered on several common themes, and CMS has taken steps to address these challenges:

- *Impact on continuing proactive data analysis investigations*: Officials from all of the ZPICs we interviewed reported that the implementation of the system represented a change in direction that limited some of their own proactive data analysis and investigations. This happened because the ZPICs were required to devote more time and resources to following up on leads from the system and less on investigations that were already under way from other sources, including earlier proactive data analysis. In addition to investigating leads from the system, the ZPICs investigate leads based on their own data analysis and cited specific advantages of their proactive investigations. Specifically, while FPS models address specific types of potential fraudulent activity, the ZPICs conduct proactive data analysis and investigations to target forms of fraud that are not addressed by those models. Additionally, ZPIC officials told us that fraudulent activity varies by region and proactive data analysis and investigations are needed to keep up with localized and emerging trends of fraud. CMS officials told us that they plan to have ZPICs continue their proactive data analysis and investigations in addition to those in response to FPS leads.

- *Certain CMS directions for using FPS*: ZPICs identified certain CMS directions for using the system that created workload challenges. For example, the agency initially directed the ZPICs to continue tracking and reevaluating providers that were determined to be nonsuspect, which led the ZPICs to expend resources investigating those providers. In response to ZPIC complaints about having to reevaluate providers determined to be nonsuspect, agency program integrity officials told us that they revised the policy so that the ZPICs only reevaluate nonsuspect providers under certain conditions and also

[19] GAO, *Results Oriented Cultures: Implementation Steps to Assist Mergers and Organizational Transformations*, GAO-03-669 (Washington, D.C.: July 2003).

modified FPS to alert ZPICs when such providers should be reexamined.

- *False positives*: ZPICs told us that certain FPS models identified and prioritized the investigation of a relatively high proportion of false positives—i.e., improper identification of suspect providers that were not engaged in fraud. Some of these false positives related to the nationwide application of models, which did not take into account localized conditions that may help explain certain provider billing patterns. For example, a physician in a rural area may provide care for beneficiaries dispersed across a large geographic range—something that would raise suspicion for a physician in an urban area. ZPICs also told us that the system sometimes prioritized leads that target forms of fraud that are not prevalent in their zone and that investigating such false positive leads has taken time away from other investigations. In response to ZPIC feedback that certain models produced a high number of false positive leads, CMS changed the way the system generates leads and how it assigns risk scores to providers identified by those models. According to program integrity officials, CMS is also considering approaches to control for geographic variations in fraud.

- *FPS functionality*: ZPICs cited challenges related to aspects of FPS's functionality. For example, when first implemented, the system only provided data directly relevant to the aberrant billing patterns associated with its leads. ZPICs, however, told us that determining whether a provider is potentially suspect requires contextual and background information, such as provider profile and billing history information. Because this information was not provided by FPS, the ZPICs had to use other sources to obtain this information. Based on this feedback, CMS updated the system so that its leads now provide users with contextual and background information on providers identified by the system.

CMS's Use of FPS Has Generally Been Consistent with Practices Identified by Private Insurers and Medicaid Programs

CMS's use of FPS has generally been consistent with key practices for using predictive analytics technologies identified by private insurers and state Medicaid programs we interviewed. The use of sophisticated predictive analytics to address health care fraud—including predictive modeling and social network analysis—is relatively new, and not all insurers and programs that we interviewed use these techniques.[20] Further, none of the insurers or programs we identified used predictive analytics to automatically deny payment of claims, and only two had processes in place to deny or suspend claims on a prepayment basis following investigations of their systems' leads. Nevertheless, the nine insurers and five Medicaid programs identified key practices for incorporating predictive analytics into their antifraud efforts, and CMS has taken steps to align FPS with such practices:

- Using a variety of data sources for predictive analytics, including public records, such as criminal, death, and corporate records, can improve results. Death records, for example, can help identify providers that submit fraudulent claims for services for dead beneficiaries. CMS has taken steps to incorporate a variety of different data into FPS. For example, the system uses information from CMS's Compromised Numbers Database to identify potentially fraudulent claims that utilize stolen provider or beneficiary identities. Additionally, program integrity officials stated that they are planning to integrate data into FPS from the agency's Automated Provider Screening system, another key information technology initiative that is intended to prevent enrollment of providers who are likely to commit Medicare fraud.[21] CMS officials stated that analysis of data provided by the screening system was under way and data from the system are expected to be integrated into FPS by the end of 2012. This planned integration with CMS's Automated Provider Screening system, which uses public records as part of the provider enrollment screening

[20] Social network analysis involves the use of public records and other data to demonstrate social linkages between individuals and entities to draw connections between individuals and providers potentially involved in fraud schemes. FPS did not include social network analysis and this report did not examine privacy or other legal or policy issues relevant to social network analysis.

[21] The Automated Provider Screening system was implemented by CMS in December 2011. This system validates data received from providers when enrolling in Medicare and identifies providers that may be at high risk for fraud based on those enrollment applications.

process, should enable FPS to risk-score providers based on certain public records.

- Social network analysis is emerging as an important tool to combat organized health care fraud since it can be used to demonstrate linkages among individuals involved in fraud schemes. One official from a state Medicaid program noted that, since organized fraud operations often move from scheme to scheme, identifying the networks of individuals involved in fraud, rather than simply limiting their ability to perpetrate certain schemes, is increasingly important. While FPS does not yet include social network analysis, CMS program integrity officials were conducting a pilot to determine how to integrate social network analysis into future model development. These officials stated that they intend to analyze and implement results of the study, as appropriate, by the end of September 2012.

- Close and continuing collaboration between those developing predictive analytics systems and the investigative staff who use the systems improves analysis and helps limit false positives. Predictive analytics systems need effective and continuous feedback on the outcomes of investigations so that they can be refined and updated to better target fraudulent activity and reduce false positives. For example, investigative staff can guide the development of predictive models by providing information on emerging fraud schemes that they encounter during the course of their investigations. CMS has coordinated with the ZPICs to develop and refine FPS models. For example, CMS has obtained ZPICs' input on emerging trends in potentially fraudulent activity to generate new ideas for FPS models. According to CMS program integrity and ZPIC officials, ZPIC staff with experience and expertise investigating particular types of fraud have been involved in developing FPS models. After models have been implemented, ZPICs have provided feedback on issues or challenges that they have encountered, which has subsequently been used by CMS to refine and update the models.

- Collaboration with external stakeholders, including other insurers and government health programs, can aid in the detection of fraudulent providers and leverages resources. Such collaborations enable information sharing about bad actors and emerging fraud schemes, which can be effective because providers engaged in fraud often do not target just one company or government program, but attempt to defraud many insurers and programs. CMS, along with other agencies involved in ensuring Medicare program integrity—specifically the HHS OIG, the Department of Justice, and the Federal Bureau of

Investigation—have established a collaborative partnership with a number of private insurers and anti-health care fraud associations. A CMS program integrity official told us that CMS's experiences with FPS will inform the information it shares with stakeholders and should enable the agency to share lessons learned regarding its use of predictive analytics with private insurers.

- Publicizing the use of predictive analytics technologies may deter providers from committing fraud. Providers may be more reluctant to commit fraud if they are aware of analytic systems in place to detect aberrant billing patterns. CMS has taken steps to publicize FPS among providers. For example, CMS distributed an article on its use of the system to the provider community[22] and presented information on the system at a regional fraud summit and at other meetings attended by medical societies and other national healthcare organizations.

While CMS's use of FPS has generally been consistent with key practices, we identified one area as a potential concern. Private insurers and state Medicaid programs reported that they leverage the results of predictive analytics to address broader program vulnerabilities—service- or system-specific weaknesses that can lead to payment errors—including vulnerabilities that are exploited for fraud. For example, private insurers and state Medicaid programs reported using predictive analytics to identify and close prepayment edit gaps and coverage policy loopholes that are exploited by providers for fraud, such as lack of utilization limits for certain services.[23] Addressing vulnerabilities identified through the use of FPS may be a concern, however, given previously identified weaknesses in CMS's processes for addressing vulnerabilities in the Medicare program. In 2010, we found weaknesses in CMS's processes to address Medicare program vulnerabilities through edits or other corrective actions, and CMS concurred with our recommendations that the agency take steps to promptly evaluate and resolve these vulnerabilities. A December 2011 report by the HHS OIG also found that, by January 2011,

[22] See "Predictive Modeling Analysis of Medicare Claims," *MLN Matters* (2011), accessed Oct. 27, 2011, http://www.cms.gov/mlnmattersarticles/downloads/se1133.pdf.

[23] Private insurers also noted that predictive analytics also identified vulnerabilities related to waste and abuse.

CMS had not resolved or had not taken significant action to resolve nearly 90 percent of the vulnerabilities identified by ZPICs in 2009.[24]

CMS Has Not Defined and Measured Quantifiable Benefits and Performance Goals for FPS

The Clinger-Cohen Act of 1996 and OMB guidance emphasize the need for agencies to forecast expected financial benefits of major investments in information technology and measure actual benefits accrued through implementation. Doing so is essential to ensure that these investments produce improvements in mission performance.[25]

In addition to the need to define and measure financial benefits, as part of capital planning and investment control processes,[26] OMB requires agencies to define and report progress against outcome-based performance measures that reflect goals and objectives of information technology programs.[27] In doing so, agencies are required to set ambitious but achievable targets once performance measures are defined,[28] establish milestones for meeting performance goals and targets that illustrate how progress toward accomplishing goals will be monitored by the agency, and conduct post-implementation reviews of systems to

[24] See GAO, *Medicare Recovery Audit Contracting: Weaknesses Remain in Addressing Vulnerabilities to Improper Payments, Although Improvements Made to Contractor Oversight*, GAO-10-143 (Washington, D.C., Mar. 31, 2010), and HHS OIG, *Addressing Vulnerabilities Reported by Medicare Benefit Integrity Contractors*, OEI-03-10-00500 (Washington, D.C.: December 2011). This figure includes vulnerabilities that were identified by PSCs.

[25] Clinger-Cohen Act of 1996, 40 U.S.C. sections 11101-11704, and OMB, Circular No. A-130, *Management of Federal Information Resources* (Nov. 30, 2000).

[26] OMB requires agencies to complete this process for major information technology investments as defined by an agency's capital planning and investment control process. HHS defines major information technology investments as programs requiring special management attention because they have estimated life-cycle costs equal to or greater than $50 million or because of their importance to the mission or function of the agency.

[27] OMB, *Guide to the Performance Assessment Rating Tool* (Washington, D.C.: January 29, 2007).

[28] OMB defines a baseline as the approved work breakdown structure, costs, schedule, and performance goals for a given investment. A baseline is the starting point from which gains are measured and targets are set. A target is used to refer to an improved level of performance needed to achieve a goal.

determine whether or not objectives were met and estimated benefits realized.[29]

OMB further requires agencies to submit business plans that address these elements throughout the life of a major investment to, among other things, provide a basis for measuring performance and identify who is accountable for deliverables of the program.[30] The data reported in the plans are available to the public and are intended to provide Congress with critical information needed to conduct oversight of, and make decisions regarding, federal agencies' investments in information technology programs.

With regard to FPS, CMS had not yet defined an approach for quantifying the financial benefits expected from the use of the system. CPI officials stated that they had not yet determined how to quantify and measure financial benefits from the system, but that they intend to do so in the future. These officials stated their intention was to measure benefits based on savings resulting from the system's contributions to the agency's efforts to prevent payments of fraudulent claims. However, while CMS could potentially quantify financial benefits resulting from the amount of suspended payments or other administrative actions based on the results of FPS, the capability of the system that could provide benefits through the suspension of payments had not yet been implemented. The officials further acknowledged the difficulty with determining benefits or return on the agency's investment in FPS in part because fraudulent providers' knowledge of CMS's use of the system could likely have a deterrent effect and, as intended, prevent fraudulent activity from occurring. In these cases, the amount of costs avoided would be unknown. FPS program officials told us that they were conducting a study to determine ways to quantify these benefits and planned to include this information in the implementation report that CMS was required to issue to Congress by September 30, 2012. However, as of October 10, 2012, the agency had not yet issued the report.

[29] OMB, Circular A-130, Transmittal Memorandum No. 4, "Management of Federal Information Resources, 8. b (1)" (Washington, D.C.: Nov. 28, 2000).

[30] OMB requires agencies to report at least annually on updates to plans or business cases for certain information technology investments and monthly to update the status of agency efforts to complete planned activities and meet established performance metrics.

In addition to the difficulties associated with the agency's efforts to quantify financial benefits of implementing FPS, CMS has not established or reported to OMB outcome-based performance measures, targets, and milestones for gauging the system's contribution to meeting its fraud prevention goals. As part of the fraud prevention program's long-term vision to stop payment on high-risk claims,[31] program officials defined two goals:

- implement predictive modeling and other analytic technology systems capable of reporting alerts based on risk scores applied to near-real-time claims data, beginning July 1, 2011, and
- identify potentially fraudulent payments before final payment is authorized by CMS.

As required, CMS initially reported to OMB performance measures, targets, and milestones in a September 2011 investment plan.[32] According to program officials, FPS stakeholders, such as CPI program managers, provided input into the development of these measures. However, in further discussions, the FPS business process owner stated that the information that had been reported to OMB in the 2011 plan did not reflect the current direction of the FPS program and that another plan was developed in January 2012. The official stated that this latter plan was being used to manage the investment and that it identified different performance goals and measures than the one submitted to OMB. Specifically, whereas the plan submitted to OMB included as a performance target 60 new models to be developed and implemented in the system by July 2012, the revised plan, which had not been submitted to OMB, identified the implementation of 40 new models for the same time frame.

[31] In spring 2011, CMS established its National Fraud Prevention Program. Among other things, the vision for the program was to integrate key information technology initiatives—e.g.., FPS and the Automated Provider Screening system—designed to support the agency's overall effort to improve its ability to prevent fraud in the Medicare program.

[32] Federal agencies' information technology investment plans are made publicly available through an OMB website, referred to as the "IT Dashboard." Information posted on this site reflects dates certain activities occur, such as updates to and departmental review of agency data.

Furthermore, the revised plan that CMS is using to manage the FPS investment does not define outcome-based performance measures that could be used to gauge progress toward the agency's goal to identify potentially fraudulent payments of claims. Some of the performance measures defined in this plan—such as the number of trouble tickets generated or number of defects—can be used to monitor system performance, but cannot be used to measure progress toward meeting program goals. In this regard, CMS did not define measures or targets for meeting them that reflect the extent to which the system identifies potentially fraudulent claims. For example, such measures could track the number of ASRs in certain risk categories that result in investigations, revocations, payment suspensions, or other administrative actions that support the agency's goal to prevent Medicare fraud. However, measures such as these, along with targets and milestones for meeting them, had not yet been defined.

Program officials stated that they intended to refine the performance measures, targets, and milestones and submit a new FPS investment plan to OMB in June 2012; however, they have not yet done so, and it is unclear when they intend to submit a revised plan or refine the performance measures. The officials also said that they intended to present performance measures in the report that CMS was required to issue to Congress by the end of September 2012. However, as noted above, the agency has not yet issued the report. In refining the performance measures for the system, it will be important that the measures be based on desired outcomes of the overall fraud prevention program to help the agency gauge improvements attributable to the implementation of FPS.

Further, while CMS's technical review board requested FPS officials to conduct a post-implementation review 6 months after the system was implemented, program officials have not yet done so. These types of reviews are to be conducted to evaluate information systems after they become operational and determine whether their implementation resulted in financial savings, changes in practices, and effectiveness in serving stakeholders. In this regard, quantifiable financial benefits and measureable performance targets and goals provide information needed to conduct post-implementation reviews of systems. However, agency officials do not yet have the information needed to conduct such a review since they have not yet defined and measured any financial benefits realized as a result of using the system, or ways to measure its overall performance. Until the agency conducts its post-implementation review of FPS, CMS will be unable to determine whether the use of the system is beneficial and effective in supporting program integrity analysts' ability to prevent payment of fraudulent claims, a key component of the agency's broader strategy for preventing fraud in the Medicare program.

Conclusions

As part of its efforts to move beyond a pay-and-chase approach to recovering fraudulent payments, CMS has taken important steps toward preventing fraud by implementing FPS in response to the Small Business Jobs Act of 2010. By integrating the system with its existing claims processing systems, the agency has provided most of the intended users an additional tool for conducting analysis of data soon after claims are submitted for payment and the ability to detect and investigate potentially fraudulent billing patterns more quickly. As implemented, the system provides functionality that supports program integrity analysts across the country in their efforts to identify and prevent payment of potentially fraudulent claims until they are determined to be valid.

CMS has also used FPS as a tool to better coordinate efforts with ZPICs, the contractors primarily responsible for investigating fraud. For example, CMS officials have directed the ZPICs to prioritize the investigation of high-risk leads generated by the system and to use the system as part of their processes for investigating potentially fraudulent claims and providers. Accordingly, the ZPICs we examined have integrated the use and outcomes of the system into their zone-specific processes. While they noted both advantages and initial challenges associated with the implementation of FPS, CMS has taken steps to address those challenges. Specifically, program integrity officials solicited users' feedback and incorporated it into the system design to improve the functionality and use of the system. Further, while the use of sophisticated predictive analytics to address health care fraud is relatively new, CMS's use of FPS has generally been consistent with key practices identified by private insurers and state Medicaid programs we interviewed. However, these entities leverage the results of predictive analytics to address broader program vulnerabilities, such as closing prepayment edit gaps and policy loopholes, and CMS could benefit from using the results of FPS to address vulnerabilities in the Medicare program that could lead to fraudulent payments.

Despite these efforts, agency officials have not yet implemented functionality in the system needed to suspend payment of high-risk claims until they are determined through further investigation to be valid, and have not yet developed detailed schedules for doing so. Additionally, they have not yet determined ways to define and measure financial benefits of using the system, nor have they established outcome-based performance measures and milestones for meeting the performance targets that reflect the goals of the agency's fraud prevention program. Until such performance indicators are established, FPS officials will continue to lack the information needed to conduct a post-implementation review of the system to determine its benefits and effectiveness in supporting program integrity analysts' efforts to identify potentially fraudulent claims and providers. Furthermore, CMS officials, OMB, and Congress may lack important information needed to determine whether the use of the system contributes to the agency's goal of predicting and preventing the payment of potentially fraudulent claims for Medicare services. In this regard, the contribution of FPS to the agency's effectiveness in preventing fraud will remain unknown.

Recommendations for Executive Action

To help ensure that the implementation of FPS is successful in helping the agency meet the goals and objectives of its fraud prevention strategy, we are recommending that the Secretary of HHS direct the Administrator of CMS to

- define quantifiable benefits expected as a result of using the system, along with mechanisms for measuring them, and
- describe outcome-based performance targets and milestones that can be measured to gauge improvements to the agency's fraud prevention initiatives attributable to the implementation of FPS.

CMS officials could consider addressing these two recommendations when reporting to Congress on the savings attributable to FPS's first year of implementation.

We are also recommending that the Secretary direct the Administrator of CMS to

- develop schedules for completing plans to further integrate FPS with the claims payment processing systems that identify all resources and activities needed to complete tasks and that consider risks and obstacles to the program, and
- conduct a post-implementation review of the system to determine whether it is effective in providing the expected financial benefits and supporting CMS's efforts to accomplish the goals of its fraud prevention program.

Agency Comments and Our Evaluation

In written comments on a draft of this report, signed by HHS's Assistant Secretary for Legislation (and reprinted in appendix II), the department stated that it appreciated the opportunity to review the report prior to its publication. Additionally, HHS stated that it concurred with all of our recommendations and identified steps that CMS officials were taking to implement them. Among these were actions to define quantifiable benefits realized as a result of using FPS, which agency officials intend to report in their first annual report to Congress. HHS also stated that CMS intends to establish outcome-base performance targets and milestones based on the first year of the system's implementation and use, and that the agency has developed detailed plans and schedules such as those we described for further integrating FPS into the Medicare fee-for-service claims payment processing systems. Finally, the department stated that CMS plans to conduct a formal post-implementation review of the system in accordance with the agency's standard operating procedures. If these and other actions that HHS identified are effectively implemented to address our recommendations, CMS should be better positioned to meet the goals and objectives of its fraud prevention program. HHS also provided technical comments on the draft report, which we 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 interested congressional committees, the Secretary of Health and Human Services, the Administrator of the Centers for Medicare and Medicaid Services, and other interested parties. In addition, this report will be available at no charge on the GAO website at http://www.gao.gov.

If you or your staff have any questions about this report, please contact us at (202) 512-6304 or melvinv@gao.gov, or (202) 512- 5154 or 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 who made key contributions to this report are listed in appendix III.

Sincerely yours,

Valerie C. Melvin

Valerie C. Melvin
Director
Information Management and Technology Resources Issues

Kathleen M. King

Kathleen King
Director
Health Care

Appendix I: Objectives, Scope, and Methodology

The objectives of our review were to (1) determine the status of implementation and use of the Centers for Medicare and Medicaid Services' (CMS) Fraud Prevention System (FPS) within the agency's existing information technology infrastructure, (2) describe how the agency uses FPS to identify and investigate potentially fraudulent payments, (3) assess how the agency's use of FPS compares to private insurers' and Medicaid programs' practices, and (4) determine the extent to which CMS defined and measured benefits and performance goals for the system and has identified and met milestones for achieving those goals.

To determine the status of the implementation and use of the predictive analytics system, we reviewed FPS program management and planning documentation and held discussions with officials responsible for developing and implementing the system, including the business process owner, information technology specialist, and contracting officer, and with users of the system. Specifically, to assess the extent to which FPS had been developed and implemented, we compared the functionality implemented to date to plans defined in project management artifacts such as statements of work, work breakdown structures, and system release notes. To determine the number of system users of FPS, we held discussions with CMS officials about the intended users of the system and obtained data describing the targeted user population and the actual number of users each month from July 2011, when the system was implemented, through April 2012.

To assess the extent to which FPS had been integrated within CMS's existing information technology infrastructure, we compared system documentation to agency modernization plans and other planning documents, such as project schedules and documents describing the system's data flows and sources. To supplement this information, we discussed with agency officials their plans for and management of the FPS program. We also interviewed officials with the Office of Information Services and the Center for Program Integrity (CPI) to discuss the agency's information technology modernization plan and the extent to which elements of the plan have been implemented, the use of agency systems as data sources for FPS, and how FPS is integrated into the existing IT infrastructure. Additionally, we viewed a demonstration of FPS given by CPI officials during our site visit to their offices. We focused our analysis on the extent to which CMS implemented and used the predictive analytics system within the existing IT infrastructure.

To describe how the agency uses FPS to identify and investigate potentially fraudulent payments, we observed demonstrations of FPS during site visits to CMS and Zone Program Integrity Contractors (ZPIC)—the primary users who are contractors responsible for conducting fraud investigations in specific geographical zones and for following up on leads generated by the system—and interviewed CMS program integrity staff responsible for implementing FPS. We conducted site visits in two zones and interviewed officials from four other zones—including the legacy Program Safeguard Contractors that are being replaced by ZPICs—representing all fully operational program integrity contractors at the time of our audit work. The locations for the site visits were selected based on (1) whether the ZPIC had been fully implemented for more than a year and (2) if the ZPIC covered geographical areas that have been identified by CMS as having high levels of fraud risk. During these discussions we sought to, among other things, understand how the contractors use FPS, the benefits and challenges associated with their use of the system, and how it had been integrated with other tools and approaches used to detect potential fraud. We also reviewed relevant documents, such as the CMS Medicare Program Integrity Manual, statements of work for ZPICs, CMS guidance and directions to the contractors, and educational materials related to FPS.

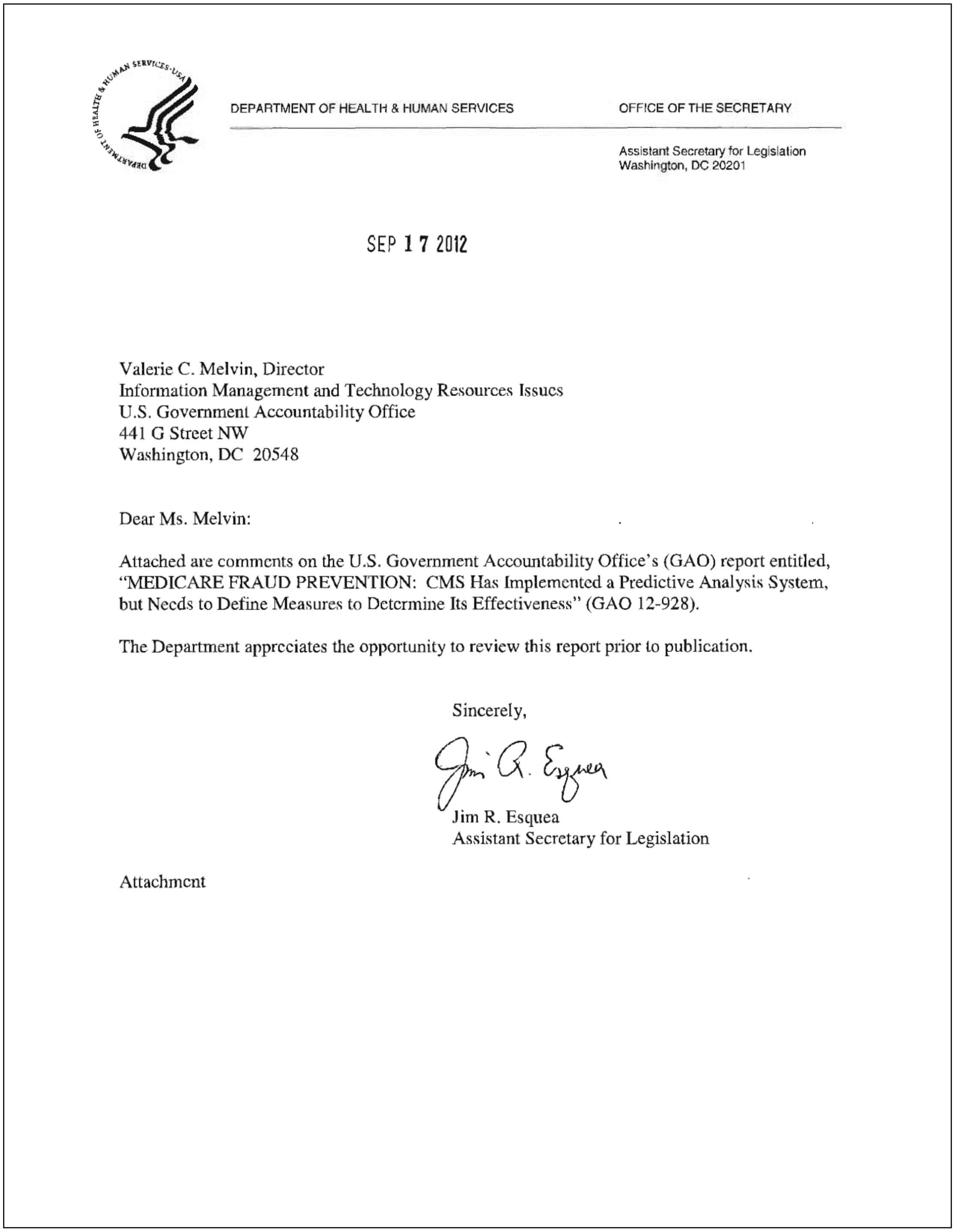
To assess how the agency's use of FPS compares to private insurers' and Medicaid programs' practices, we examined the use of similar systems by private health insurers and Medicaid programs. To identify these users, we employed a methodology often referred to as "snowball sampling": an iterative process whereby at each interview with knowledgeable stakeholders, we solicited names of insurers and Medicaid programs that were using predictive analytics until we had coverage of a broad range of users and perspectives. Our observations are based on interviews with five state Medicaid programs and nine private insurance companies. We selected a nonprobability sample of stakeholders to interview and, therefore, the information gathered from key stakeholders is not generalizable beyond the individuals we interviewed; however, the interviews provided insights into issues pertaining to all three objectives. While not all users employed sophisticated predictive analytics—including predictive modeling and social network analysis—at the time of our interviews, they all had experience with data analytics and were able to provide insights into process-oriented strategies for incorporating analytics into their antifraud efforts. Our understanding of predictive analytics and its use was also informed by trade journal articles and interviews with system vendors and health insurance and antifraud organizations.

To determine the extent to which CMS defined and measured benefits and performance goals for the system and identified and met milestones for achieving those goals, we reviewed requirements established by the Office of Management and Budget (OMB) for agencies' management of information technology investments and for reporting the status of those investments. We assessed efforts taken by CMS officials to meet OMB's requirements. Specifically, we discussed with the FPS business owner and other program officials the steps they had taken and plan to take in efforts to define ways to measure financial and other quantifiable benefits of the system. We also discussed with them their approach to and processes for developing performance measures, targets, and milestones to determine the extent to which the system was producing outcomes that supported the agency's fraud prevention strategies and goals. Additionally, we reviewed agency-wide strategic plans and program planning documents, and assessed the extent to which the system's performance plans and objectives supported efforts to achieve the goals defined by these plans. We also examined reports submitted to OMB that included information about the system's expected performance, and interviewed program officials about steps the agency had taken to achieve the goals and objectives.

For each of the objectives, we assessed the reliability of the data we obtained from interviews with agency officials and users by comparing them to documents describing FPS's program plans and status, information technology infrastructure, system design specifications, system usage reports, and performance goals and measures. We found the data sufficiently reliable for the purposes of this review.

We conducted this performance audit from October 2011 to October 2012 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.

Appendix II: Comments from the Department of Health and Human Services



DEPARTMENT OF HEALTH & HUMAN SERVICES

OFFICE OF THE SECRETARY

Assistant Secretary for Legislation
Washington, DC 20201

SEP 17 2012

Valerie C. Melvin, Director
Information Management and Technology Resources Issues
U.S. Government Accountability Office
441 G Street NW
Washington, DC 20548

Dear Ms. Melvin:

Attached are comments on the U.S. Government Accountability Office's (GAO) report entitled, "MEDICARE FRAUD PREVENTION: CMS Has Implemented a Predictive Analysis System, but Needs to Define Measures to Determine Its Effectiveness" (GAO 12-928).

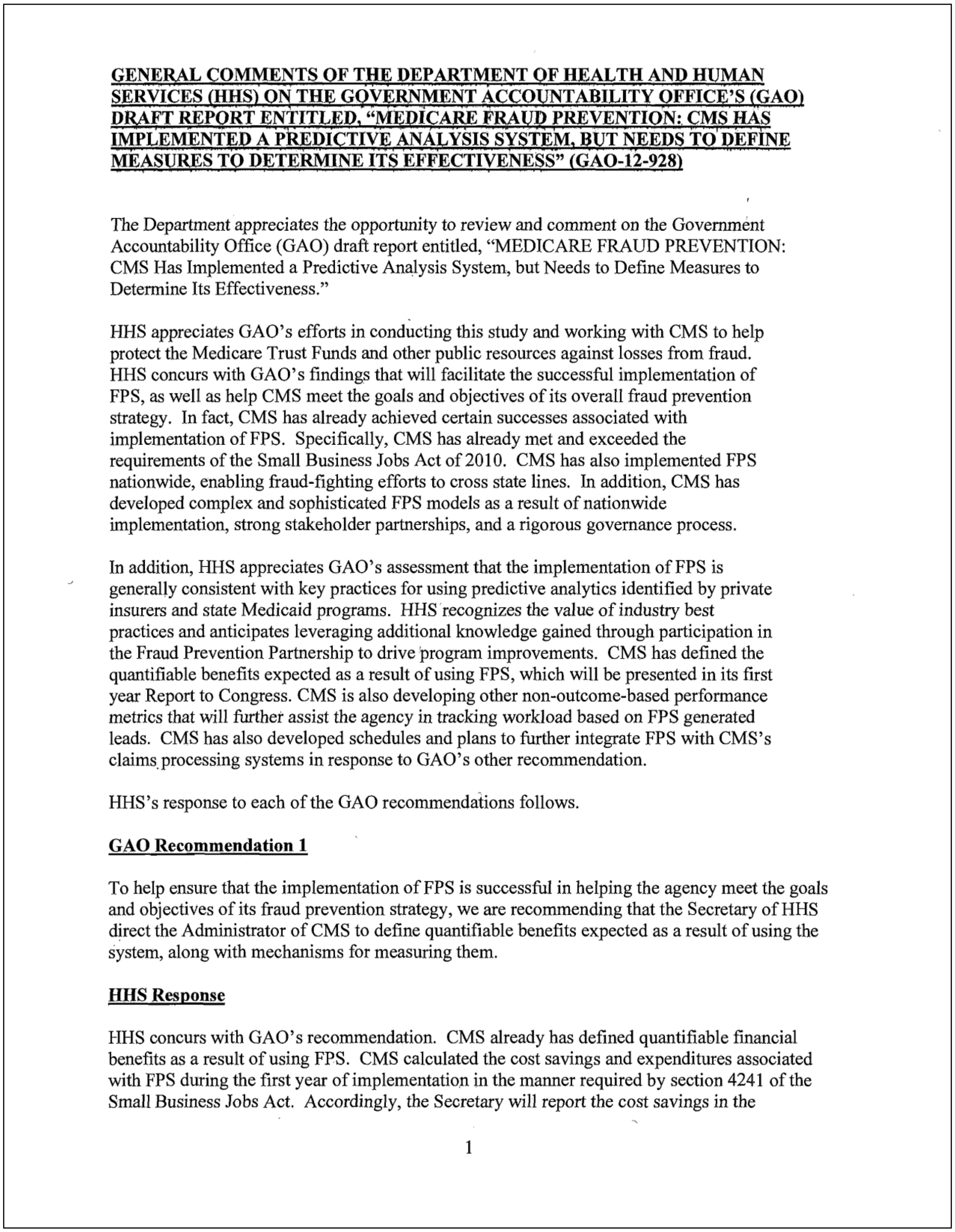
The Department appreciates the opportunity to review this report prior to publication.

Sincerely,

Jim R. Esquea

Jim R. Esquea
Assistant Secretary for Legislation

Attachment



GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "MEDICARE FRAUD PREVENTION: CMS HAS IMPLEMENTED A PREDICTIVE ANALYSIS SYSTEM, BUT NEEDS TO DEFINE MEASURES TO DETERMINE ITS EFFECTIVENESS" (GAO-12-928)

The Department appreciates the opportunity to review and comment on the Government Accountability Office (GAO) draft report entitled, "MEDICARE FRAUD PREVENTION: CMS Has Implemented a Predictive Analysis System, but Needs to Define Measures to Determine Its Effectiveness."

HHS appreciates GAO's efforts in conducting this study and working with CMS to help protect the Medicare Trust Funds and other public resources against losses from fraud. HHS concurs with GAO's findings that will facilitate the successful implementation of FPS, as well as help CMS meet the goals and objectives of its overall fraud prevention strategy. In fact, CMS has already achieved certain successes associated with implementation of FPS. Specifically, CMS has already met and exceeded the requirements of the Small Business Jobs Act of 2010. CMS has also implemented FPS nationwide, enabling fraud-fighting efforts to cross state lines. In addition, CMS has developed complex and sophisticated FPS models as a result of nationwide implementation, strong stakeholder partnerships, and a rigorous governance process.

In addition, HHS appreciates GAO's assessment that the implementation of FPS is generally consistent with key practices for using predictive analytics identified by private insurers and state Medicaid programs. HHS recognizes the value of industry best practices and anticipates leveraging additional knowledge gained through participation in the Fraud Prevention Partnership to drive program improvements. CMS has defined the quantifiable benefits expected as a result of using FPS, which will be presented in its first year Report to Congress. CMS is also developing other non-outcome-based performance metrics that will further assist the agency in tracking workload based on FPS generated leads. CMS has also developed schedules and plans to further integrate FPS with CMS's claims processing systems in response to GAO's other recommendation.

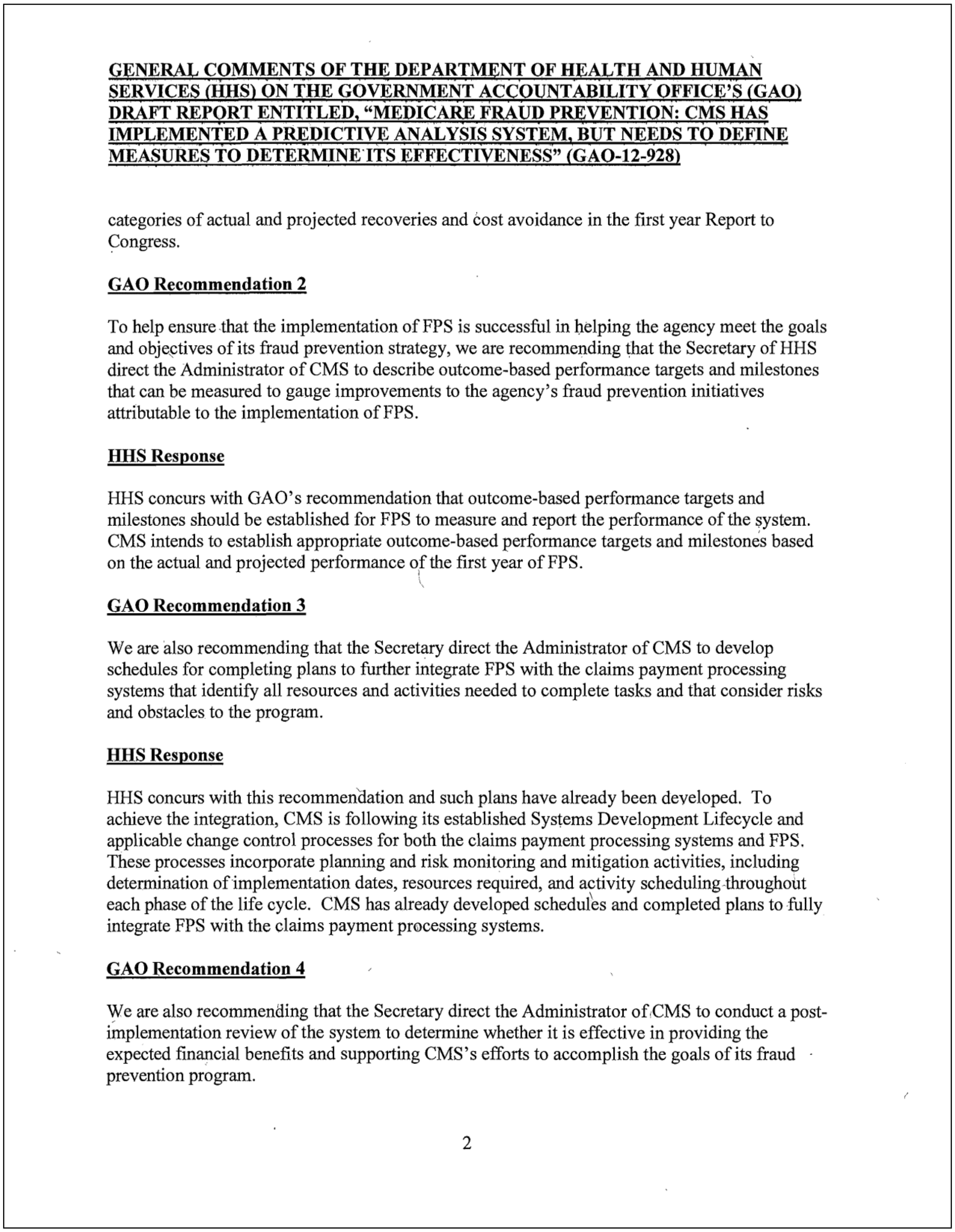
HHS's response to each of the GAO recommendations follows.

GAO Recommendation 1

To help ensure that the implementation of FPS is successful in helping the agency meet the goals and objectives of its fraud prevention strategy, we are recommending that the Secretary of HHS direct the Administrator of CMS to define quantifiable benefits expected as a result of using the system, along with mechanisms for measuring them.

HHS Response

HHS concurs with GAO's recommendation. CMS already has defined quantifiable financial benefits as a result of using FPS. CMS calculated the cost savings and expenditures associated with FPS during the first year of implementation in the manner required by section 4241 of the Small Business Jobs Act. Accordingly, the Secretary will report the cost savings in the



GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "MEDICARE FRAUD PREVENTION: CMS HAS IMPLEMENTED A PREDICTIVE ANALYSIS SYSTEM, BUT NEEDS TO DEFINE MEASURES TO DETERMINE ITS EFFECTIVENESS" (GAO-12-928)

categories of actual and projected recoveries and cost avoidance in the first year Report to Congress.

GAO Recommendation 2

To help ensure that the implementation of FPS is successful in helping the agency meet the goals and objectives of its fraud prevention strategy, we are recommending that the Secretary of HHS direct the Administrator of CMS to describe outcome-based performance targets and milestones that can be measured to gauge improvements to the agency's fraud prevention initiatives attributable to the implementation of FPS.

HHS Response

HHS concurs with GAO's recommendation that outcome-based performance targets and milestones should be established for FPS to measure and report the performance of the system. CMS intends to establish appropriate outcome-based performance targets and milestones based on the actual and projected performance of the first year of FPS.

GAO Recommendation 3

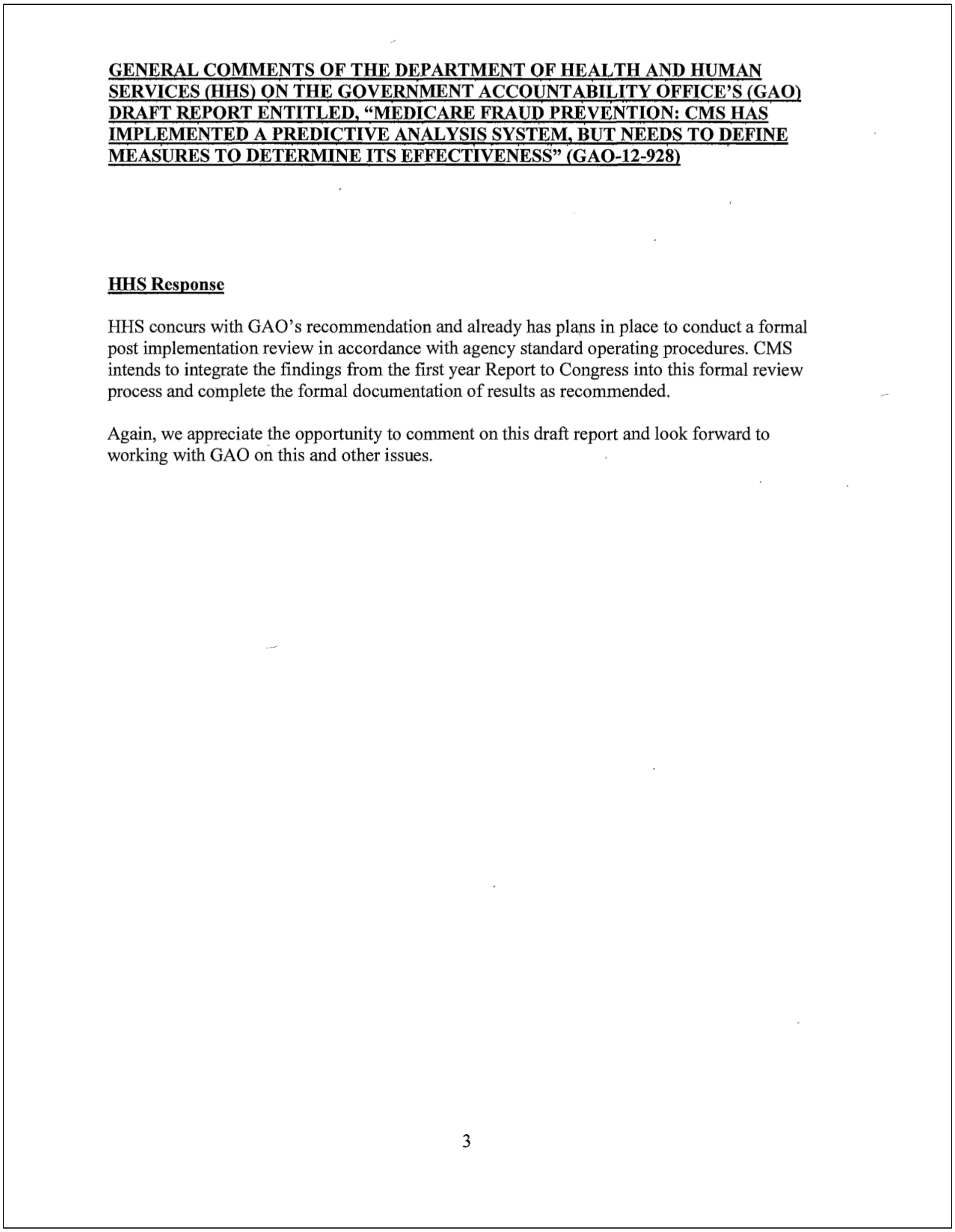
We are also recommending that the Secretary direct the Administrator of CMS to develop schedules for completing plans to further integrate FPS with the claims payment processing systems that identify all resources and activities needed to complete tasks and that consider risks and obstacles to the program.

HHS Response

HHS concurs with this recommendation and such plans have already been developed. To achieve the integration, CMS is following its established Systems Development Lifecycle and applicable change control processes for both the claims payment processing systems and FPS. These processes incorporate planning and risk monitoring and mitigation activities, including determination of implementation dates, resources required, and activity scheduling throughout each phase of the life cycle. CMS has already developed schedules and completed plans to fully integrate FPS with the claims payment processing systems.

GAO Recommendation 4

We are also recommending that the Secretary direct the Administrator of CMS to conduct a post-implementation review of the system to determine whether it is effective in providing the expected financial benefits and supporting CMS's efforts to accomplish the goals of its fraud prevention program.



GENERAL COMMENTS OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES (HHS) ON THE GOVERNMENT ACCOUNTABILITY OFFICE'S (GAO) DRAFT REPORT ENTITLED, "MEDICARE FRAUD PREVENTION: CMS HAS IMPLEMENTED A PREDICTIVE ANALYSIS SYSTEM, BUT NEEDS TO DEFINE MEASURES TO DETERMINE ITS EFFECTIVENESS" (GAO-12-928)

HHS Response

HHS concurs with GAO's recommendation and already has plans in place to conduct a formal post implementation review in accordance with agency standard operating procedures. CMS intends to integrate the findings from the first year Report to Congress into this formal review process and complete the formal documentation of results as recommended.

Again, we appreciate the opportunity to comment on this draft report and look forward to working with GAO on this and other issues.

Appendix III: GAO Contacts and Staff Acknowledgments

GAO Contacts

Valerie C. Melvin, (202) 512-6304 or melvinv@gao.gov

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

Staff Acknowledgments

In addition to the contacts named above, Teresa F. Tucker, Assistant Director; Thomas A. Walke, Assistant Director; Neil J. Doherty; Michael A. Erhardt; Amanda C. Gill; Lee A. McCracken; Thomas E. Murphy; Monica Perez-Nelson; Kate F. Nielsen; and Eden Savino made key contributions to this report.

(310972)

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, 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.

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