



Testimony

Before the Subcommittee on Oversight
and Investigations, Committee on Energy
and Commerce, House of Representatives

For Release on Delivery
Expected at 9:30 a.m. EDT
Friday, June 8, 2012

MEDICARE

Progress Made to Deter Fraud, but More Could Be Done

Statement of Kathleen M. King
Director, Health Care

To access this report
electronically, scan this
QR Code.

Don't have a QR code
reader? Several are
available for free online.



G A O

Accountability * Integrity * Reliability



Highlights of [GAO-12-801T](#), a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

Why GAO Did This Study

GAO has designated Medicare as a high-risk program. Since 1990, every two years GAO has provided Congress with an update on this program, which highlights government operations that are at high risk for waste, fraud, abuse, mismanagement or in need of broad reform. Medicare has been included in this program 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. 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. Reducing fraud could help rein in the escalating costs of the program.

This statement focuses on the progress made and important steps to be taken by CMS and its program integrity contractors to reduce fraud in Medicare. These contractors perform functions such as screening and enrolling providers, detecting and investigating potential fraud, and identifying improper payments and vulnerabilities that could lead to payment errors. This statement is based on relevant GAO products and recommendations issued from 2004 through 2012 using a variety of methodologies, such as analyses of Medicare claims, review of relevant policies and procedures, and interviews with officials.

View [GAO-12-801T](#). For more information, contact Kathleen M. King at (202) 512-7114 or kingk@gao.gov.

June 8, 2012

MEDICARE

Progress Made to Deter Fraud, but More Could Be Done

What GAO Found

The Centers for Medicare & Medicaid Services (CMS)—the agency that administers Medicare—has made progress in implementing several key strategies GAO identified in prior work as helpful in protecting Medicare from fraud; however, important actions that could help CMS and its program integrity contractors combat fraud remain incomplete.

Provider Enrollment: GAO's previous work found persistent weaknesses in Medicare's enrollment standards and procedures that increased the risk of enrolling entities intent on defrauding the program. CMS has strengthened provider enrollment—for example, in February 2011, CMS designated three levels of risk—high, moderate, and limited—with different screening procedures for categories of providers at each level. However, CMS has not completed other actions, including implementation of some relevant provisions of the Patient Protection and Affordable Care Act (PPACA). Specifically, CMS has not (1) determined which providers will be required to post surety bonds to help ensure that payments made for fraudulent billing can be recovered, (2) contracted for fingerprint-based criminal background checks, (3) issued a final regulation to require additional provider disclosures of information, and (4) established core elements for provider compliance programs.

Pre- and Post-payment Claims Review: GAO had previously found that increased efforts to review claims on a prepayment basis can prevent payments from being made for potentially fraudulent claims, while improving systems used by CMS and its contractors to review claims on a post-payment basis could better identify patterns of potentially fraudulent billing for further investigation. CMS has controls in Medicare's claims-processing systems to determine if claims should be paid, denied, or reviewed further. These controls require timely and accurate information about providers that GAO has previously recommended that CMS strengthen. GAO is currently examining CMS's new Fraud Prevention System, which uses analytic methods to examine claims before payment to develop investigative leads for Zone Program Integrity Contractors (ZPIC), the contractors responsible for detecting and investigating potential fraud. Additionally, CMS could improve its post-payment claims review to identify patterns of fraud by incorporating prior GAO recommendations to develop plans and timelines for fully implementing and expanding two information technology systems it developed.

Robust Process to Address Identified Vulnerabilities: Having mechanisms in place to resolve vulnerabilities that lead to erroneous payments is critical to effective program management and could help address fraud. Such vulnerabilities are service- or system-specific weaknesses that can lead to payment errors—for example, providers receiving multiple payments as a result of incorrect coding. GAO has previously identified weaknesses in CMS's process for addressing identified vulnerabilities and the Department of Health and Human Services' Office of Inspector General recently reported on CMS's inaction in addressing vulnerabilities identified by its contractors, including ZPICs. GAO is evaluating the current status of the process for assessing and developing corrective actions to address vulnerabilities.

Mr. Chairman, Ranking Member, and Other Members of the Committee:

I am pleased to be here today to discuss our work regarding fraud in the Medicare program, Medicare contractors' roles in detecting and preventing fraud, and provisions in recent laws and agency actions that may help address this problem.¹ Fraud involves an intentional act or representation to deceive with the knowledge that the action or representation could result in gain. Although there have been convictions for multi-million dollar schemes that defrauded the Medicare program, the extent of the problem is unknown. There are no reliable estimates of the extent of fraud in the Medicare program or for the health care industry as a whole. By its very nature, fraud is difficult to detect, as those involved are engaged in intentional deception. For example, fraud may involve providers submitting a claim with false documentation for services not provided, while the claim on its face may appear valid. Fraud also can involve efforts to hide ownership of companies or kickbacks to obtain beneficiary information. Although the full extent of the problem is unknown, it is clear that the Medicare program is vulnerable to fraud, which contributes to Medicare's fiscal problems. Reducing fraud could help rein in the escalating costs of the program.

We have repeatedly designated Medicare as a high-risk program, as its complexity and susceptibility to payment errors from various causes, added to its size, have made it vulnerable to loss.² As one example, the fee-for-service (FFS) portion of the Medicare program processes over a billion claims a year from about 1.5-million providers and suppliers; working to ensure that those payments are accurate is a complex, ongoing task. Medicare has many individual vulnerabilities, which are

¹Medicare is the federally financed health insurance program for persons age 65 or over, certain individuals with disabilities, and individuals with end-stage renal disease. Medicare Parts A and B are known as Medicare fee-for-service (FFS). Medicare Part A covers hospital and other inpatient stays. Medicare Part B is optional, and covers hospital outpatient, physician, and other services. Medicare beneficiaries have the option of obtaining coverage for Medicare services from private health plans that participate in Medicare Advantage—Medicare's managed care program—also known as Part C. All Medicare beneficiaries may purchase coverage for outpatient prescription drugs under Part D, either as a stand-alone benefit or as part of a Medicare Advantage plan.

²In 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. Medicare has been included among such programs since 1990. See GAO, *High-Risk Series: An Update*, [GAO-11-278](#) (Washington, D.C.: February 2011). http://www.gao.gov/highrisk/risks/insurance/medicare_program.php.

service- or system-specific weaknesses that can lead to payment errors, including those due to fraud.³ If the Centers for Medicare & Medicaid Services (CMS), the agency within the Department of Health and Human Services (HHS) that administers the program, suspects that providers or suppliers are billing fraudulently, it can take action, including suspending claims payment, revoking billing privileges, or referring cases to law enforcement for investigation.⁴ Further, it can impose a moratorium on new enrollment of providers or suppliers.⁵ Since 1997, Congress has provided funds specifically for activities to address fraud, as well as waste and abuse,⁶ in Medicare and other federal health care programs. In addition, Congress created the Medicare Integrity Program to conduct activities to reduce fraud, waste, abuse, and improper payments.⁷ In 2010, Congress passed the Patient Protection and Affordable Care Act (PPACA), which provided additional funding for such efforts and set a number of new requirements specific to Medicare.⁸ Furthermore, the

³CMS defines vulnerabilities to the Medicare program as issues that can lead to fraud, waste, or abuse, which can either be specific, such as providers receiving multiple payments as a result of incorrect coding for a service, or general and programwide, such as weaknesses in online application processes.

⁴In this testimony, the term *provider* includes entities such as hospitals or physicians, and *supplier* means an entity that supplies Medicare beneficiaries with durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS) such as walkers and wheelchairs.

⁵Enrolling as a provider or supplier in Medicare allows an entity to provide services or equipment to beneficiaries and bill for those services.

⁶Waste includes inaccurate payments for services, such as unintentional duplicate payments. Abuse represents actions inconsistent with acceptable business or medical practices.

⁷An improper payment is any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. This definition includes any payment to an ineligible recipient, any payment for an ineligible good or service, any duplicate payment, any payment for a good or service not received (except where authorized by law), and any payment that does not account for credit for applicable discounts. Improper Payments Elimination and Recovery Act of 2010, Pub. L. No. 111-204, § 2(e), 124 Stat. 2224, 2227 (codified at 31 U.S.C. § 3321 note).

⁸Pub. L. No. 111-148, 124 Stat. 119 (2010), as amended by Health Care and Education Reconciliation Act of 2010 (HCERA), Pub. L. No. 111-152, 124 Stat. 1029, which we refer to collectively as PPACA. The provisions discussed in this statement are generally located in sections 6401 through 6411 and 10603 and 10605 of PPACA, as well as sections 1303 and 1304 of HCERA.

Small Business Jobs Act of 2010⁹ established new Medicare fee-for-service claims review requirements and provided funding to implement these requirements.

My testimony today focuses on the progress made and steps that remain to be taken by CMS and its program integrity contractors to reduce fraud in Medicare. CMS contractors perform a number of key program integrity functions, such as screening and enrolling providers, detecting and investigating potential fraud, and identifying improper payments and vulnerabilities that could lead to payment errors. This testimony is informed by 8 years of our work on Medicare fraud, waste, abuse, and improper payments. I will focus on several key strategies CMS can undertake to help reduce fraud discussed in our prior work from 2004 to 2012, specifically:¹⁰

- strengthening provider enrollment standards and procedures,
- improving pre- and post-payment claims review, and
- developing a robust process for addressing identified vulnerabilities.

The products on which this statement is based were developed by using a variety of methodologies, including analyses of Medicare claims, review of relevant policies and procedures, interviews with agency officials and other stakeholders, and site visits.¹¹ The work on which these products were based was conducted 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.

⁹Pub. L. No. 111-240, § 4241, 124 Stat. 2504, 2599.

¹⁰These strategies were among those identified in our June 2010 testimony as critical to helping prevent fraud, waste, and abuse in Medicare. See GAO, *Medicare Fraud, Waste, and Abuse: Challenges and Strategies for Preventing Improper Payments*, [GAO-10-844T](#) (Washington, D.C.: June 15, 2010). A list of related products appears at the end of this statement.

¹¹The products listed at the end of this statement contain detailed information on the methodologies used in our work.

CMS Has Made Progress in Strengthening Provider Enrollment, but Further Actions Are Needed

CMS has made progress strengthening provider enrollment to try to better ensure that only legitimate providers and suppliers are allowed to bill Medicare. However, CMS has not completed other actions that could help prevent individuals intent on fraud from enrolling, including implementation of some relevant PPACA provisions.

Past CMS Efforts to Strengthen Provider Enrollment

Our previous work found persistent weaknesses in Medicare’s enrollment standards and procedures that increased the risk of enrolling entities intent on defrauding the Medicare program.¹² We, CMS, and the HHS Office of Inspector General (OIG) have previously identified two types of providers whose services and items are especially vulnerable to improper payments and fraud—home health agencies (HHA) and suppliers of durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS). We found weaknesses in oversight of these providers’ and suppliers’ enrollment. For example, in 2008, we identified weaknesses when we created two fictitious DMEPOS companies, which were subsequently enrolled by CMS’s contractor and given permission to begin billing Medicare.¹³ In 2009, we found that CMS’s contractors were not requiring HHAs to resubmit enrollment information for re-verification every 5 years as required by CMS.¹⁴

To strengthen the Medicare enrollment process, in 2006 CMS began requiring all providers and suppliers—including those that order HHA services or DMEPOS for beneficiaries to be enrolled in Medicare. The agency also required all providers and suppliers to report their National Provider Identifiers (NPI) on enrollment applications, which can help

¹²See GAO, *Medicare: CMS’s Program Safeguards Did Not Deter Growth in Spending for Power Wheelchairs*, [GAO-05-43](#) (Washington, D.C.: Nov. 17, 2004); *Medicare: More Effective Screening and Stronger Enrollment Standards Needed for Medical Equipment Suppliers*, [GAO-05-656](#) (Washington, D.C.: Sept. 22, 2005); *Medicare: Improvements Needed to Address Improper Payments for Medical Equipment and Supplies*, [GAO-07-59](#) (Washington, D.C.: Jan. 31, 2007); and *Medicare: Improvements Needed to Address Improper Payments in Home Health*, [GAO-09-185](#) (Washington, D.C.: Feb. 27, 2009).

¹³GAO, *Medicare: Covert Testing Exposes Weaknesses in the Durable Medical Equipment Supplier Screening Process*, [GAO-08-955](#) (Washington, D.C.: July 3, 2008).

¹⁴[GAO-09-185](#).

address fraud because providers and suppliers must submit either their Social Security Number or their employer identification number and state licensing information to obtain an NPI.¹⁵ In 2007, CMS initiated the first phase of a Medicare competitive-bidding program for DMEPOS.¹⁶ This program requires suppliers' bids to include new financial documentation for the year prior to submitting the bids. Because CMS can now disqualify suppliers based in part on new scrutiny of their financial documents, competitive bidding can help reduce fraud. Finally, in 2010, CMS also required that all DMEPOS suppliers be accredited by a CMS-approved accrediting organization to ensure that they meet certain quality standards. Such accreditation also increased scrutiny of these businesses.

CMS Has Taken Action on Certain PPACA Provider Enrollment Provisions

PPACA authorized CMS to implement several actions to strengthen provider enrollment. As of April 2012, the agency has completed some of these actions.

Screening Provider Enrollment Applications by Risk Level: CMS and OIG issued a final rule with comment period in February 2011 to implement some of the new screening procedures required by PPACA.¹⁷ CMS designated three levels of risk—high, moderate, and limited—with different screening procedures for categories of Medicare providers at each level. Providers in the high-risk level are subject to the most rigorous

¹⁵The Health Insurance Portability and Accountability Act of 1996 required that HHS adopt standards for unique health identifiers. CMS adopted the NPI as the standard unique health identifier for its health care providers and suppliers in its final rule: *HIPAA Administrative Simplification: Standard Unique Health Identifier for Health Care Providers*, 69 *Fed. Reg.* 3434 (Jan. 23, 2004). Consistent with the NPI final rule, beginning in 2006, the Medicare program required providers and suppliers to report their NPIs on their enrollment applications.

¹⁶Competitive bidding is a process in which suppliers of medical equipment and supplies compete for the right to provide their products on the basis of established criteria, such as quality and price.

¹⁷*Medicare, Medicaid, and Children's Health Insurance Programs; Additional Screening Requirements, Application Fees, Temporary Enrollment Moratoria, Payment Suspensions and Compliance Plans for Providers and Suppliers*, 76 *Fed. Reg.* 5862 (Feb. 2, 2011). In discussing the final rule, CMS noted that Medicare had already employed a number of the screening practices described in PPACA to determine if a provider is in compliance with federal and state requirements to enroll or to maintain enrollment in the Medicare program.

screening.¹⁸ To determine which providers to place in these risk levels, CMS considered issues such as past occurrences of improper payments and fraud among different categories of providers. Based in part on our work and that of the OIG, CMS designated newly enrolling HHAs and DMEPOS suppliers as high risk and designated other providers at lower levels. (See table 1.) Providers at all risk levels are screened to verify that they meet specific requirements established by Medicare such as having current licenses or accreditation and valid Social Security numbers.¹⁹ High- and moderate-risk providers are additionally subject to unannounced site visits. Further, depending on the risks presented, PPACA authorizes CMS to require fingerprint-based criminal history checks, and the posting of surety bonds for certain providers.²⁰ CMS may also provide enhanced oversight for specific periods for new providers and for initial claims of DMEPOS suppliers.

¹⁸PPACA specified that the enhanced-screening procedures would apply to new providers and suppliers beginning 1 year after the date of enactment and to currently enrolled providers and suppliers 2 years after that date.

¹⁹Screening may include verification of the following: Social Security number; NPI; National Practitioner Databank licensure; whether the provider has been excluded from federal health care programs by the OIG; taxpayer identification number; and death of an individual practitioner, owner, authorized official, delegated official, or supervising physician.

²⁰A surety bond is a three-party agreement in which a company, known as a surety, agrees to compensate the bondholder if the bond purchaser fails to keep a specified promise.

Table 1: Categories of Medicare Providers and Suppliers Designated by Risk Level for Enrollment Screening

Risk level	Categories of Medicare providers and suppliers
Limited	Physician or nonphysician practitioners and medical groups or clinics, with the exception of physical therapists and physical therapy groups. Ambulatory surgical centers, competitive acquisition programs/Part B vendors, end-stage renal disease facilities, federally qualified health centers, histocompatibility laboratories, ^a Indian Health Service facilities, mammography screening centers, mass immunization roster billers, ^b organ procurement organizations, pharmacies newly enrolling or revalidating, radiation therapy centers, religious nonmedical health care institutions, rural health clinics, skilled nursing facilities, and hospitals, including critical access hospitals.
Moderate	Ambulance suppliers, community mental health centers, comprehensive outpatient rehabilitation facilities, hospice organizations, independent diagnostic testing facilities, independent clinical laboratories, portable X-ray suppliers, currently enrolled (revalidating) home health agencies, and physical therapy, including physical therapy groups.
High	Prospective (newly enrolling) home health agencies and prospective (newly enrolling) suppliers of durable medical equipment, prosthetics, orthotics, and supplies.

Source: GAO analysis of CMS Final Rule with Comment Period, *Medicare, Medicaid, and Children's Health Insurance Programs: Additional Screening Requirements, Applications Fees, Temporary Enrollment Moratoria, Payment Suspensions and Compliance Plans for Providers and Suppliers*, 76 Fed. Reg. 5862 (Feb. 2, 2011).

^aHistocompatibility laboratories provide evaluations of certain genetic data and pertinent patient immunologic risk factors to allow clinician and patient to make decisions about whether transplantation is in the patient's best interest.

^bMass immunization roster billers are providers and suppliers that enroll in the Medicare program to offer influenza (flu) vaccinations to a large number of individuals, and these entities must be properly licensed in the states in which they plan to operate influenza clinics.

CMS indicated that the agency will continue to review the criteria for its screening levels on an ongoing basis and would publish changes if the agency decided to update the assignment of screening levels for categories of Medicare providers. This may become necessary because fraud is not confined to HHAs and DMEPOS suppliers. We are currently examining the types of providers involved in fraud cases investigated by the OIG and the Department of Justice (DOJ), which may help illuminate risk to the Medicare program from different types of providers. Further, in their 2011 annual report on the Health Care Fraud and Abuse Control Program, DOJ and HHS reported convictions or other legal actions, such as exclusions or civil monetary penalties, against several types of Medicare providers other than DMEPOS suppliers and HHAs, including pharmacists, orthopedic surgeons, infusion and other types of medical clinics, and physical therapy services.²¹ CMS also has established triggers for adjustments to an individual provider's risk level. For example, CMS regulations state that an individual provider or supplier at the

²¹ *The Department of Health and Human Services and the Department of Justice Health Care Fraud and Abuse Control Program Annual Report for Fiscal Year 2011* (Washington, D.C.: February 2012).

limited- or moderate-risk level that has had its billing privileges revoked by a Medicare contractor within the last 10 years and is attempting to re-enroll, would move to the high-risk level for screening.

New National Enrollment Screening and Site Visit Contractors: In a further effort to strengthen its enrollment processes, CMS contracted with two new entities at the end of 2011 to assume centralized responsibility for automated screening of provider and supplier enrollment and for conducting site visits of providers.

- **Automated-screening contractor.** In December 2011, the new contractor began to establish systems to conduct automated screening of providers and suppliers to ensure they meet Medicare eligibility criteria (such as valid licensure, accreditation, a valid NPI, and no presence on the OIG list of providers and suppliers excluded from participating in federal health care programs).²² Prior to the implementation of this new automated screening, such screening was done manually for the 30,000 enrollees each month by CMS's Medicare Administrative Contractors (MAC), which enroll Medicare providers, and the National Supplier Clearinghouse (NSC), which enrolls DMEPOS suppliers. According to CMS, the old screening process was neither efficient nor timely. CMS officials said that in 2012, the automated-screening contractor began automated screening of the licensure status of all currently enrolled Medicare providers and suppliers. The agency said it expects the automated-screening contractor to begin screening newly enrolling providers and suppliers later this year. CMS expects that the new, national contractor will enable better monitoring of providers and suppliers on a continuous basis to help ensure they continue to meet Medicare enrollment requirements. The new screening contractor will also help the MACs and the NSC maintain enrollment information in CMS's Provider Enrollment Chain and Ownership System (PECOS)—a database that contains details on enrolled providers and suppliers. In addition, CMS officials said the automated-screening contractor is developing an individual risk score for each provider or supplier, similar to a credit risk score. Although these individual scores are not currently used to determine an individual provider's placement in a

²²Licensure is a mandatory process by which a state government grants permission to an individual practitioner or health care organization to engage in an occupation or profession.

risk level, CMS indicated that this risk score may be used eventually as additional risk criteria in the screening process.

- **Site visits for all providers designated as moderate and high risk.** Beginning in February 2012, a single national site-visit contractor began conducting site visits of moderate- and high-risk providers to determine if sites are legitimate and the providers meet certain Medicare standards.²³ The contractor collects the same information from each site visit, including photographic evidence that will be available electronically through a Web portal accessible to CMS and its other contractors. The national site-visit contractor is expected to validate the legitimacy of these sites. CMS officials told us that the contractor will provide consistency in site visits across the country, in contrast to CMS relying on different MACs to conduct any required site visits.

CMS Has Not Completely Implemented Some PPACA Enrollment Provisions

Implementation of other enrollment screening actions authorized by PPACA that could help CMS reduce the enrollment of providers and suppliers intent on defrauding the Medicare program remains incomplete, including:

- **Surety bond**—PPACA authorizes CMS to require a surety bond for certain types of at-risk providers, which can be helpful in recouping erroneous payments. CMS officials expect to issue a proposed rule to require surety bonds as conditions of enrollment for certain other types of providers. Extending the use of surety bonds to these new entities would augment a previous statutory requirement for DMEPOS suppliers to post a surety bond at the time of enrollment.²⁴ CMS

²³Starting March 25, 2011, CMS required the MACs to conduct site visits for categories of providers and suppliers designated as moderate and high risk. The national site-visit contractor assumed these responsibilities in 2012. The NSC will continue to conduct site visits related to provider enrollment of DMEPOS suppliers. In addition, CMS at times exercises its authority to conduct a site visit or requests its contractors to conduct a site visit for any Medicare provider or supplier.

²⁴42 U.S.C. § 1395m(a)(16)(B). As of October 2009, DMEPOS suppliers were required to obtain and submit a surety bond in the amount of at least \$50,000. A DMEPOS surety bond is a bond issued by an entity guaranteeing that a DMEPOS supplier will fulfill its obligation to Medicare. If the obligation is not met, the surety bond is paid to Medicare. *Medicare Program; Surety Bond Requirement for Suppliers of Durable Medical Equipment, Prosthetics, Orthotics, and Supplies (DMEPOS)*, 74 Fed. Reg. 166 (Jan. 2, 2009).

issued final instructions to its MACs, effective February 2012, for recovering DMEPOS overpayments through surety bonds. CMS officials reported that as of April 19, 2012, they had issued notices to 20 surety bond companies indicating intent to collect funds, but had not collected any funds as of that date.

- **Fingerprint-based criminal background checks**—CMS officials told us that they are working with the Federal Bureau of Investigation to arrange contracts to help conduct fingerprint-based criminal background checks of high-risk providers and suppliers. On April 13, 2012, CMS issued a request for information regarding the potential solicitation of a single contract for Medicare provider and supplier fingerprint-based background checks. The agency expects to have the contract in place before the end of 2012.
- **Providers and suppliers disclosure**—CMS officials said the agency is reviewing options to include in regulations for increased disclosures of prior actions taken against providers and suppliers enrolling or revalidating enrollment in Medicare, such as whether the provider or supplier has been subject to a payment suspension from a federal health care program.²⁵ In April 2012, agency officials indicated that they were not certain when the regulation would be published. CMS officials noted that the additional disclosure requirements are complicated by provider and supplier concerns about what types of information will be collected, what CMS will do with it, and how the privacy and security of this information will be maintained.
- **Compliance and ethics program**—CMS officials said that the agency was studying criteria found in OIG model plans as it worked to address the PPACA requirement that the agency establish the core

²⁵At the time of initial enrollment or revalidation of enrollment, PPACA requires providers and suppliers to disclose any current or previous affiliation with another provider or supplier that has uncollected debt; has been or is subject to a payment suspension under a federal health care program; has been excluded from participation under Medicare, Medicaid, or the State Children's Health Insurance Program; or has had its billing privileges denied or revoked. Pub. L. No. 111-148, § 6401(a)(4), 124 Stat. 119, 740 (2010).

elements of compliance programs for providers and suppliers.²⁶ As of April 2012, CMS did not have a projected target date for implementation.

Additional Action May Help Better Identify Potential Fraud through Pre- and Post-Payment Claims Review

Increased efforts to review claims on a prepayment basis can better prevent payments that should not be made, while improving systems used to review claims on a post-payment basis could better identify patterns of fraudulent billing for further investigation.

Additional Efforts to Improve Prepayment Claims Review May Help Reduce Fraud

Having robust controls in claims payment systems to prevent payment of problematic claims can help reduce loss. As claims go through Medicare's electronic claims payment systems, they are subjected to automated prepayment controls called "edits," instructions programmed in the systems to prevent payment of incomplete or incorrect claims. Some edits use provider enrollment information, while others use information on coverage or payment policies, to determine if claims should be paid. Most of these controls are fully automated; if a claim does not meet the criteria of the edit, it is automatically denied. Other prepayment edits are manual; they flag a claim for individual review by trained staff who determine if it should be paid. Due to the volume of claims, CMS has reported that less than 1 percent of Medicare claims are subject to manual medical record review by trained staff.

Having effective pre-payment edits that deny claims for ineligible providers and suppliers depends on having timely and accurate information about them, such as whether the providers are currently enrolled and have the appropriate license or accreditation to provide specific services. We previously recommended that CMS take action to

²⁶A compliance program is an internal set of policies, processes, and procedures that a provider organization implements to help it act ethically and lawfully. In this context, a compliance program is intended to help provider and supplier organizations prevent and detect violations of Medicare laws and regulations. CMS has used the phrase "compliance and ethics program" and indicated it may base its program on the seven elements of effective compliance and ethics programs found in the U.S. Federal Sentencing Guidelines Manual.

ensure the timeliness and accuracy of PECOS—the database that maintains Medicare provider and supplier enrollment information. We noted that weaknesses in PECOS data may result in CMS making improper payments to ineligible providers and suppliers.²⁷ These weaknesses are related to the frequency with which CMS’s contractors update enrollment information and the timeliness and accuracy of information obtained from outside entities, such as state licensing boards, the OIG, and the Social Security Administration’s Death Master File, which contains information on deceased individuals that can be used to identify deceased providers in order to terminate those providers’ Medicare billing privileges. These sources vary in the ease in which CMS contractors have been able to access their data and the frequency with which they are updated. CMS has indicated that its new national-screening contractor should improve the timeliness and accuracy of the provider and supplier information in PECOS by centralizing the process, increasing automation of the process, continuously checking databases, and incorporating new sources of data, such as financial, business, tax, and geospatial data. However, it is too soon to tell if these efforts will better prevent payments to ineligible providers and suppliers.

Having effective edits to implement coverage and payment policies before payment is made can also help to deter fraud. The Medicare program has defined categories of items and services eligible for coverage and excludes from coverage items or services that are determined not to be “reasonable and necessary for the diagnosis and treatment of an illness or injury or to improve functioning of a malformed body part.”²⁸ CMS and its contractors set policies regarding when and how items and services will be covered by Medicare, as well as coding and billing requirements for payment, which also can be implemented in the payment systems through edits. We have previously found Medicare’s payment systems did not have edits for items and services unlikely to be provided in the normal course of medical care.²⁹ CMS has since implemented edits to flag such claims—called Medically Unlikely Edits. We are currently assessing Medicare’s prepayment edits based on coverage and payment policies, including the Medically Unlikely Edits.

²⁷ [GAO-12-351](#).

²⁸ 42 U.S.C. § 1395y(a)(1)(A).

²⁹ [GAO-07-59](#).

Additionally, suspending payments to providers suspected of fraudulent billing can be an effective tool to prevent excess loss to the Medicare program while suspected fraud is being investigated. For example, in March 2011, the OIG testified that payment suspensions and pre-payment edits on 18 providers and suppliers stopped the potential loss of more than \$1.3 million submitted in claims by these individuals. Furthermore, HHS recently reported that it imposed payment suspensions on 78 home health agencies in conjunction with arrests related to a multimillion-dollar health care fraud scheme. 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.³⁰ CMS officials reported that the agency had imposed 212 payment suspensions since the regulations implementing the PPACA provisions took effect. Agency officials indicated that almost half of these suspensions were imposed this calendar year, representing about \$6 million in Medicare claims.

We are currently evaluating a new CMS effort, the Fraud Prevention System (FPS), which uses predictive analytic technologies to analyze FFS claims on a prepayment basis to develop investigative leads for CMS's Zone Program Integrity Contractors (ZPIC), the contractors responsible for detecting and investigating potential fraud.³¹ The Small Business Jobs Act of 2010 requires CMS to use predictive analytic technologies both to identify and to prevent improper payments under Medicare FFS.³² The law requires these predictive analytic technologies to be used to review claims for potential fraud by identifying unusual or

³⁰CMS is required to consult with the HHS OIG in determining whether a credible allegation of fraud exists. Based on how CMS used its previous payment suspension authority, in November 2010, the OIG found weaknesses in CMS's implementation of payment suspensions that could lead to delays in the suspension process. Such delays would allow payments to continue to providers suspected of fraud. Specifically, the OIG found that CMS's guidance to its contractors on procedures for implementing payment suspensions was incomplete and inconsistent. Although the OIG made no recommendations, it suggested that these weaknesses could be addressed through CMS rulemaking pursuant to PPACA.

³¹CMS is replacing its legacy Program Safeguard Contractors (PSC) with seven ZPICs. While the PSCs were responsible for program integrity for specific parts of Medicare, such as Part A, the ZPICs are responsible for Medicare's fee-for-service program integrity in their geographic zones. For simplicity, we refer to these program integrity contractors as ZPICs throughout the testimony.

³²Pub. L. No. 111-240, § 4241, 124 Stat. 2504, 2599.

suspicious patterns or abnormalities in Medicare provider networks, claims billing patterns, and beneficiary utilization. According to CMS, FPS may enhance CMS's ability to identify potential fraud because it analyzes large numbers of claims from multiple data sources nationwide simultaneously before payment is made, thus allowing CMS to examine billing patterns across geographic regions for those that may indicate fraud. The results of FPS are used by the ZPICs to initiate investigations that could result in payment suspensions, implementation of automatic claim denials, identification of additional prepayment edits, or the revocation of Medicare billing privileges. CMS began using FPS to screen all FFS claims nationwide prior to payment as of June 30, 2011, and CMS has been directing the ZPICs to investigate high priority leads generated by the system. Because FPS is relatively new and we have not completed our work, it is too soon to determine whether FPS will improve CMS's ability to address fraud. Questions have also been raised about CMS's ability to adequately assess ZPICs' performance and we have been asked to examine CMS's management of the ZPICs, including criteria used by CMS to evaluate their effectiveness.

"Bust-out" fraud schemes in which providers or suppliers suddenly bill very high volumes of claims to obtain large payments from Medicare could be addressed by adding a prepayment edit. Such an edit would set thresholds to stop payment for atypically rapid increases in billing thus helping them to stem losses from these schemes. In our prior work on DMEPOS, we recommended that CMS require its contractors to develop thresholds for unexplained increases in billing and use them to develop pre-payment controls that could suspend these claims for further review before payment.³³ CMS officials told us that they are currently considering developing analytic models in FPS that could help CMS and ZPICs identify and address billing practices suggestive of bust outs.

³³See GAO, *2012 Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue*. [GAO-12-342SP](#) (Washington, D.C.: Feb. 28, 2012) and [GAO-07-59](#).

**Actions Needed to
Improve Use of Systems
Intended for Post-payment
Claims Review**

Further actions are needed to improve use of two CMS information technology systems that could help CMS and program integrity contractors identify fraud after claims have been paid.³⁴

- The Integrated Data Repository (IDR) became operational in September 2006 as a central data store of Medicare and other data needed to help CMS's program integrity staff, ZPICs, and other contractors prevent and detect improper payments of claims. However, we found IDR did not include all the data that were planned to be incorporated by fiscal year 2010, because of technical obstacles and delays in funding. Further, as of December 2011 the agency had not finalized plans or developed reliable schedules for efforts to incorporate these data, which could lead to additional delays.
- One Program Integrity (One PI) is a Web portal intended to provide CMS staff, ZPICs, and other contractors with a single source of access to data contained in IDR, as well as tools for analyzing those data. While One PI is operational, we reported in December 2011 that CMS had trained few program integrity analysts and that the system was not being widely used.

GAO recommended that CMS take steps to finalize plans and reliable schedules for fully implementing and expanding the use of both IDR and One PI. Although the agency told us in April 2012 that it had initiated activities to incorporate some additional data into IDR and expand the use of One PI, such as training more ZPIC and other staff, it has not fully addressed our recommendations.

³⁴GAO, *Fraud Detection Systems: Centers for Medicare and Medicaid Services Needs to Ensure More Widespread Use*, [GAO-11-475](#) (Washington, D.C.: June 30, 2011).

A Robust Process to Address Identified Vulnerabilities Could Help Reduce Fraud

Having mechanisms in place to resolve vulnerabilities that lead to improper payments is critical to effective program management and could help address fraud.³⁵ A number of different types of program integrity contractors are responsible for identifying and reporting vulnerabilities to CMS. However, our work and the work of OIG have shown weaknesses in CMS's processes to address vulnerabilities identified by these contractors.

CMS's Recovery Audit Contractors (RAC) are specifically charged with identifying improper payments and vulnerabilities that could lead to such payment errors. However, in our March 2010 report on the RAC demonstration program, we found that CMS had not established an adequate process during the demonstration or in planning for the national program to ensure prompt resolution of such identified vulnerabilities in Medicare; further, the majority of the most significant vulnerabilities identified during the demonstration were not addressed.³⁶ We therefore recommended that CMS develop and implement a corrective action process that includes policies and procedures to ensure the agency promptly (1) evaluates findings of RAC audits, (2) decides on the appropriate response and a time frame for taking action based on established criteria, and (3) acts to correct the vulnerabilities identified.³⁷

Our recommendations will not be fully addressed until CMS has put policies and procedures in place that will lead the agency to act promptly to correct identified vulnerabilities. In December 2011, the OIG similarly found that CMS lacked procedures to ensure that vulnerabilities identified

³⁵We have reported that an agency should have policies and procedures to ensure that (1) the findings of all audits and reviews are promptly evaluated, (2) decisions are made about the appropriate response to these findings, and (3) actions are taken to correct or resolve the issues promptly. These are all aspects of internal control, which is the component of an organization's management that provides reasonable assurance that the organization achieves effective and efficient operations, reliable financial reporting, and compliance with applicable laws and regulations. Internal control standards provide a framework for identifying and addressing major performance challenges and areas at greatest risk for mismanagement. GAO, *Internal Control Standards: Internal Control Management and Evaluation Tool*, [GAO-01-1008G](#) (Washington, D.C.: August 2001).

³⁶GAO, *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).

³⁷[GAO-10-143](#).

by other contractors were resolved.³⁸ CMS had not resolved or taken significant action to resolve 38 of 44 vulnerabilities (86 percent) reported in 2009 by ZPICs. Only 1 vulnerability had been fully resolved by January 2011.³⁹ The OIG made several recommendations, including that CMS have written procedures and time frames to assure that vulnerabilities were resolved. CMS has indicated that it is now tracking vulnerabilities identified from several types of contractors through a single vulnerability tracking process. We are currently examining aspects of CMS's vulnerability tracking process and will be reporting on it soon.

Concluding Observations

Although CMS has taken some important steps to identify and prevent fraud, including implementing provisions in PPACA and the Small Business Jobs Act, more remains to be done to prevent making erroneous Medicare payments due to fraud. In particular, we have found CMS could do more to strengthen provider enrollment screening to avoid enrolling those intent on committing fraud, improve pre- and post-payment claims review to identify and respond to patterns of suspicious billing activity more effectively, and identify and address vulnerabilities to reduce the ease with which fraudulent entities can obtain improper payments. It is critical that CMS implement and make full use of new authorities granted by recent legislation, as well as incorporate recommendations made by us, as well as the OIG in these areas. Moving from responding once fraud has already occurred to preventing it from occurring in the first place is key to ensuring that federal funds are used efficiently and for their intended purposes.

As all of these new authorities and requirements become part of Medicare's operations, additional evaluation and oversight will be necessary to determine whether they are implemented as required and have the desired effect. We have several studies underway that assess efforts to fight fraud in Medicare and that should continue to help CMS refine and improve its fraud detection and prevention efforts. Notably, we are assessing the effectiveness of different types of pre-payment edits in

³⁸HHS-OIG, *Addressing Vulnerabilities Reported by Medicare Benefit Integrity Contractors*, OEI-03-10-00500 (December 2011).

³⁹OIG also found that CMS had not resolved or taken significant action to resolve 10 of 18 vulnerabilities (56 percent) reported in 2009 by Medicare Prescription Drug Integrity Contractors (MEDICs)—program integrity contractors for Medicare Parts C and D. Only 1 of those 18 vulnerabilities had been fully resolved by January 2011.

Medicare and of CMS's oversight of its contractors in implementing those edits to help ensure that Medicare pays claims correctly the first time. We are also examining the use of predictive analytics by CMS and the ZPICs to improve fraud prevention and detection. ZPICs play an important role in detecting and investigating fraud and identifying vulnerabilities, and FPS will likely play an increasing role in how ZPICs conduct their work. Additionally, we have work under way to identify the types of providers and suppliers currently under investigation and those that have been found to have engaged in fraudulent activities. These studies may enable us to point out additional actions for CMS that could help the agency more systematically reduce fraud in the Medicare program.

Due to the amount of program funding at risk, fraud will remain a continuing threat to Medicare, so continuing vigilance to reduce vulnerabilities will be necessary. Individuals who want to defraud Medicare will continue to develop new approaches to try to circumvent CMS's safeguards and investigative and enforcement efforts. Although targeting certain types of providers that the agency has identified as high risk may be useful, it may allow other types of providers committing fraud to go unnoticed. We will continue to assess efforts to fight fraud and provide recommendations to CMS, as appropriate, that we believe will assist the agency and its contractors in this important task. We urge CMS to continue its efforts as well.

Mr. Chairman, this concludes my prepared statement. I would be happy to answer any questions you or other members of the committee may have.

For further information about this statement, please contact Kathleen M. King at (202) 512-7114 or kingk@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Thomas Walke, Assistant Director; Michael Erhardt; Eden Savino; and Jennifer Whitworth were key contributors to this statement.

Related GAO Products

Medicare Program Integrity: CMS Continues Efforts to Strengthen the Screening of Providers and Suppliers. [GAO-12-351](#). Washington, D.C.: April 24, 2012.

Improper Payments: Remaining Challenges and Strategies for Governmentwide Reduction Efforts. [GAO-12-573T](#). Washington, D.C.: March 28, 2012.

2012 Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue. [GAO-12-342SP](#). Washington, D.C.: February 28, 2012.

Fraud Detection Systems: Centers for Medicare and Medicaid Services Needs to Expand Efforts to Support Program Integrity Initiatives. [GAO-12-292T](#). Washington, D.C.: December 7, 2011.

Medicare Part D: Instances of Questionable Access to Prescription Drugs. [GAO-12-104T](#). Washington, D.C.: October 4, 2011.

Medicare Part D: Instances of Questionable Access to Prescription Drugs. [GAO-11-699](#). Washington, D.C.: September 6, 2011.

Medicare Integrity Program: CMS Used Increased Funding for New Activities but Could Improve Measurement of Program Effectiveness. [GAO-11-592](#). Washington, D.C.: July 29, 2011.

Improper Payments: Reported Medicare Estimates and Key Remediation Strategies. [GAO-11-842T](#). Washington, D.C.: July 28, 2011.

Fraud Detection Systems: Additional Actions Needed to Support Program Integrity Efforts at Centers for Medicare and Medicaid Services. [GAO-11-822T](#). Washington, D.C.: July 12, 2011.

Fraud Detection Systems: Centers for Medicare and Medicaid Services Needs to Ensure More Widespread Use. [GAO-11-475](#). Washington, D.C.: June 30, 2011.

Medicare and Medicaid Fraud, Waste, and Abuse: Effective Implementation of Recent Laws and Agency Actions Could Help Reduce Improper Payments. [GAO-11-409T](#). Washington, D.C.: March 9, 2011.

Medicare: Program Remains at High Risk Because of Continuing Management Challenges. [GAO-11-430T](#). Washington, D.C.: March 2, 2011.

High-Risk Series: An Update. [GAO-11-278](#). Washington, D.C.: February 2011.

Medicare Part D: CMS Conducted Fraud and Abuse Compliance Plan Audits, but All Audit Findings Are Not Yet Available. [GAO-11-269R](#). Washington, D.C.: February 18, 2011.

Medicare Fraud, Waste, and Abuse: Challenges and Strategies for Preventing Improper Payments. [GAO-10-844T](#). Washington, D.C.: June 15, 2010.

Medicare Recovery Audit Contracting: Weaknesses Remain in Addressing Vulnerabilities to Improper Payments, Although Improvements Made to Contractor Oversight. [GAO-10-143](#). Washington, D.C.: March 31, 2010.

Medicare Part D: CMS Oversight of Part D Sponsors' Fraud and Abuse Programs Has Been Limited, but CMS Plans Oversight Expansion. [GAO-10-481T](#). Washington, D.C.: March 3, 2010.

Medicare: CMS Working to Address Problems from Round 1 of the Durable Medical Equipment Competitive Bidding Program. [GAO-10-27](#). Washington, D.C.: November 6, 2009.

Improper Payments: Progress Made but Challenges Remain in Estimating and Reducing Improper Payments. [GAO-09-628T](#). Washington, D.C.: April 22, 2009.

Medicare: Improvements Needed to Address Improper Payments in Home Health. [GAO-09-185](#). Washington, D.C.: February 27, 2009.

Medicare Part D: Some Plan Sponsors Have Not Completely Implemented Fraud and Abuse Programs, and CMS Oversight Has Been Limited. [GAO-08-760](#). Washington, D.C.: July 21, 2008.

Medicare: Covert Testing Exposes Weaknesses in the Durable Medical Equipment Supplier Screening Process. [GAO-08-955](#). Washington, D.C.: July 3, 2008.

Medicare: Thousands of Medicare Providers Abuse the Federal Tax System. [GAO-08-618](#). Washington, D.C.: June 13, 2008.

Medicare: Competitive Bidding for Medical Equipment and Supplies Could Reduce Program Payments, but Adequate Oversight Is Critical. [GAO-08-767T](#). Washington, D.C.: May 6, 2008.

Improper Payments: Status of Agencies' Efforts to Address Improper Payment and Recovery Auditing Requirements. [GAO-08-438T](#). Washington, D.C.: January 31, 2008.

Improper Payments: Federal Executive Branch Agencies' Fiscal Year 2007 Improper Payment Estimate Reporting. [GAO-08-377R](#). Washington, D.C.: January 23, 2008.

Medicare: Improvements Needed to Address Improper Payments for Medical Equipment and Supplies. [GAO-07-59](#). Washington, D.C.: January 31, 2007.

Medicare: More Effective Screening and Stronger Enrollment Standards Needed for Medical Equipment Suppliers. [GAO-05-656](#). Washington, D.C.: September 22, 2005.

Medicare: CMS's Program Safeguards Did Not Deter Growth in Spending for Power Wheelchairs. [GAO-05-43](#). Washington, D.C.: November 17, 2004.

Medicare: CMS Did Not Control Rising Power Wheelchair Spending. [GAO-04-716T](#). Washington, D.C.: April 28, 2004.

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

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 (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 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: 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

