United States Government Accountability Office

GAO

Report to the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate

July 2008

MEDICARE

Covert Testing Exposes Weaknesses in the Durable Medical Equipment Supplier Screening Process

GAO-08-955

July 2008

MEDICARE

Covert Testing Exposes Weaknesses in the Durable Medical Equipment Supplier Screening Process

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-08-955, a report to the Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, U.S. Senate

Why GAO Did This Study

According to the Department of Health and Human Services (HHS), schemes to defraud the Medicare program have grown more elaborate in recent years. In particular, HHS has acknowledged Centers for Medicare & Medicaid Service's (CMS) oversight of suppliers of durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS) is inadequate to prevent fraud and abuse. Specifically, weaknesses in the DMEPOS enrollment and inspection process have allowed sham companies to fraudulently bill Medicare for unnecessary or nonexistent supplies. From April 2006 through March 2007, CMS estimated that Medicare improperly paid $1 billion for DMEPOS supplies—in part due to fraud by suppliers.

Due to the committee's concern about vulnerabilities in the enrollment process, GAO used publicly available guidance to attempt to create DMEPOS suppliers, obtain Medicare billing numbers, and complete electronic test billing. GAO also reported on closed cases provided by the HHS Inspector General (IG) to illustrate the techniques used by criminals to fraudulently bill Medicare.

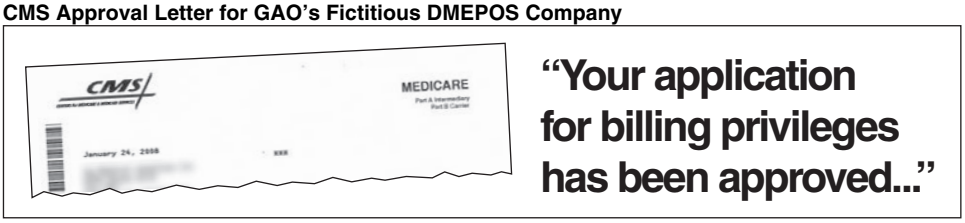
On June 18, 2008, we briefed CMS representatives on the results of our investigation. In response, they acknowledged that our covert tests illustrate gaps in oversight that still require improvement and stated that they would continue to work to strengthen the entire DMEPOS enrollment process.

To view the full product, including the scope and methodology, click on GAO-08-955. For more information, contact Gregory D. Kutz at (202) 512-6722 or kutzg@gao.gov.

What GAO Found

Investigators easily set up two fictitious DMEPOS companies using undercover names and bank accounts. GAO's fictitious companies were approved for Medicare billing privileges despite having no clients and no inventory. CMS initially denied GAO's applications in part because of this lack of inventory, but undercover GAO investigators fabricated contracts with nonexistent wholesale suppliers to convince CMS and its contractor, the National Supplier Clearinghouse (NSC), that the companies had access to DMEPOS items. The contact number GAO gave for these phony contracts rang on an unmanned undercover telephone in the GAO building. When NSC left a message looking for further information related to the contracts, a GAO investigator left a vague message in return pretending to be the wholesale supplier. As a result of such simple methods of deception, both fictitious DMEPOS companies obtained Medicare billing numbers. The following figure contains a redacted acceptance letter GAO received from CMS.

CMS Approval Letter for GAO's Fictitious DMEPOS Company



Source: CMS.

After requesting an electronic billing enrollment package and obtaining passwords from CMS, GAO investigators were then able to successfully complete Medicare's test billing process for the Virginia office. GAO could not complete test billing for the Maryland office because CMS has not sent the necessary passwords. However, if real fraudsters had been in charge of the fictitious companies, they would have been clear to bill Medicare from the Virginia office for potentially millions of dollars worth of nonexistent supplies.

Once criminals have similarly created fictitious DMEPOS companies, they typically steal or illegally buy Medicare beneficiary numbers and physician identification numbers and use them to repeatedly submit claims. In one case from HHS IG, a company received $2.2 million in payments from Medicare for supplies and services that were never delivered. The owner submitted these fraudulent claims from March 2006 through July 2006 using real beneficiary numbers and physician identification numbers that he had purchased illegally. The only employee not involved in the scheme was a secretary, who told HHS IG that there was no business activity in the office and that the owner was rarely there. Another case related to an individual who stole beneficiary numbers and physician identification numbers and submitted $5.5 million in claims for three fraudulent offices from October 2006 through March 2007. He operated one of these offices out of a utility closet containing buckets of sand mix, road tar, and a large wrench, but no medical files, office equipment, or telephone.

Contents

Figures

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

July 3, 2008

The Honorable Carl Levin
Chairman
The Honorable Norm Coleman
Ranking Member
Permanent Subcommittee on Investigations
Committee on Homeland Security and Governmental Affairs
United States Senate

Medicare, which is administered by the Department of Health and Human Services' (HHS) Centers for Medicare & Medicaid Services (CMS), helps pay for a variety of health care services and items on behalf of almost 42 million elderly and certain disabled beneficiaries. According to HHS, schemes to defraud the Medicare program have grown more elaborate in recent years, resulting in the misuse of taxpayer dollars and the misdirection of funds intended to help beneficiaries. In particular, HHS has acknowledged that there are significant vulnerabilities in CMS's oversight of suppliers of durable medical equipment, prosthetics, orthotics, and supplies (DMEPOS). Specifically, weaknesses in the DMEPOS enrollment and inspection process have allowed sham companies to fraudulently bill Medicare for unnecessary or nonexistent supplies. For example, in December 2006, the HHS Inspector General (IG) randomly visited 1,581 DMEPOS suppliers in South Florida and found that almost one-third of them did not even have an office at the business address they provided Medicare, although they had collectively submitted claims for hundreds of millions of dollars worth of supplies. In part due to fraud by suppliers, CMS estimated that, from April 2006 through March 2007, $1 billion of the $10 billion in payments Medicare made for DMEPOS supplies were improper.

To prevent fraudulent DMEPOS suppliers from entering the Medicare program, CMS developed 25 standards that suppliers must meet to be authorized to bill Medicare for health care services and items that they provide to beneficiaries.[1] These standards are intended to help ensure that

[1]See appendix I for a complete list of the standards. Three of the 25 standards were created by a 1994 statute (42 U.S.C. § 1395m(j)(1)(B)(ii)), and HHS added 4 standards related to accreditation in 2006 that were mandated by Public Law 108-173. The other 18 standards were established by regulation. The 25 standards are found at 42 C.F.R. § 424.57(c).

suppliers are legitimate businesses and properly licensed within the states they operate. CMS contracts with the National Supplier Clearinghouse (NSC) to screen potential suppliers and enroll into the Medicare program only those that comply with all 25 standards. NSC and its contractors are required to verify suppliers' compliance through on-site inspections and conduct other reviews, such as confirming that the supplier either has access to its own DMEPOS inventory or has a contract with a wholesaler. Once a DMEPOS supplier successfully completes this verification process, CMS sends the supplier an approval letter containing a Medicare billing number. To be able to submit claims to Medicare electronically, DMEPOS suppliers that opt to do their own billing also have to complete Medicare's test billing process using their billing number, Medicare beneficiary numbers, and ordering physician identification numbers.[2]

In 2005, we reported that NSC's efforts to verify compliance with the standards were insufficient because of weaknesses in procedures for checking state licensure and conducting on-site inspections.[3] As a result, CMS agreed to take a number of actions to strengthen NSC's verification procedures, including requiring NSC to conduct site inspections of DMEPOS suppliers' off-site inventory storage locations and of the wholesaler businesses that provide them with inventory through contracts.[4] Despite these reported actions, you continue to be concerned that vulnerabilities in the DMEPOS enrollment process allow fraudulent suppliers to enroll in and ultimately bill Medicare. Therefore, we agreed to test CMS's processes by attempting to create fictitious DMEPOS suppliers, obtain Medicare billing numbers, and successfully complete electronic test billing. We also agreed to develop case studies to illustrate the techniques used by criminals in recent years to fraudulently bill Medicare for DMEPOS supplies.

To complete our testing, we used publicly available guidance and software to open two DMEPOS suppliers. Because CMS has divided the country into four regions—or zones—we set up one company in Maryland (Zone

[2]DMEPOS suppliers can choose to contract with third party billing agents who do not have to complete the test billing process because these agents have their own billing software.

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

[4]Among other things, CMS agreed to require NSC to check suppliers' licenses and liability insurance each year, require NSC to conduct out-of-cycle inspections, and require the inspection of beneficiary files.

A) and one in Virginia (Zone C) so that we could determine whether the contractors conducting the Medicare application review, including visits to the companies, followed consistent review steps in each zone. To appear legitimate, we also created a series of phony documents and company policies. We then submitted applications to CMS to obtain a Medicare billing number. To complete the test billing process, we used undercover, fictitious Medicare beneficiaries, as well as physician identification numbers that we found on the Internet. It is important to note that we only used this information to complete test billing; we did not compromise the provider status of any legitimate physicians or the status of actual beneficiaries by submitting actual claims using their identification information. To demonstrate how criminals use similar techniques, we worked with the HHS IG to identify recently closed DMEPOS supplier fraud cases. We performed our undercover operation from February 2007 through June 2008 in accordance with guidelines established by the President's Council for Integrity and Efficiency.

Results in Brief

CMS approved both of our fictitious, easily created DMEPOS storefronts despite the fact that we had no clients and no inventory. Even though CMS and NSC initially denied our applications in part due to this lack of inventory, they eventually accepted the phony contracts with wholesale suppliers we created. NSC performed limited verification to confirm the authenticity of these contracts. For example, the telephone number we gave for the wholesalers rang on an unmanned undercover telephone in the GAO building. When NSC's inspector left a message on the number looking for further information related to the contracts, a GAO investigator left a vague message in return pretending to be the wholesaler. As a result of such simple methods of deception, we obtained Medicare billing privileges and billing numbers for both companies, even though we had absolutely no means of supplying prospective clients with durable medical equipment. After requesting an electronic billing enrollment package and obtaining passwords from CMS, we were then able to successfully complete Medicare's test billing process for our Virginia office; we did not complete test billing for our Maryland office because we did not receive the necessary passwords from CMS by the close of our investigation in June 2008. Based on a review of case studies we obtained from HHS IG, we believe that, had our operation continued successfully, we could have fraudulently billed Medicare for substantial sums—potentially reaching millions of dollars.

Once criminals similarly create fictitious DMEPOS companies, they typically steal or illegally buy Medicare beneficiary numbers and physician

identification numbers and use them to repeatedly submit claims. In one closed case we obtained from HHS IG, a fraudulent company billed Medicare for $4.4 million in supplies and services that were never delivered, ultimately receiving $2.2 million in payments. The owner submitted these claims from March 2006 through July 2006 using legitimate beneficiary numbers and physician identification numbers that he had purchased illegally. According to HHS, the only employee not involved in the scheme was a secretary, who told investigators that there was no business activity in the office and that the owner was rarely there. Another case relates to an individual who submitted $5.5 million in fraudulent claims from October 2006 through March 2007. This individual purchased a DMEPOS company but then submitted claims using the original owner's identity, Medicare billing number, and beneficiaries in an attempt to avoid detection by CMS. At the same time, this individual was operating two additional fraudulent DMEPOS companies—one of them located in a utility closet containing buckets of sand mix, road tar, and a large wrench (but no medical files, telephone, or other office equipment).

Background

Medicare's 25 supplier standards were introduced to deter individuals intent on committing fraud from entering the program and to safeguard Medicare beneficiaries by ensuring that suppliers were qualified. The 25 standards apply to a variety of business practices and establish certain requirements and prohibitions (see app. I for a list of the standards). For example, the standards require suppliers to have a physical facility on an appropriate site that is accessible to beneficiaries and to CMS, with stated business hours clearly posted. The following are the most pertinent standards for the purposes of this report:

- **Standard 1:** Operate business and furnish Medicare-covered items in compliance with all applicable federal and state licensure and regulatory requirements.
- **Standard 4:** Fill orders for equipment or supplies using its own inventory or by contracting with other companies. If the supplier contracts with other companies, it must provide copies of the contracts upon request.
- **Standard 7:** Maintain a physical facility that contains space for storing business records including the supplier's delivery, maintenance, and beneficiary communication records.

- **Standard 8:** Permit CMS to conduct on-site inspections. In addition, the supplier's location must be accessible during reasonable business hours to beneficiaries and to CMS, and must maintain a visible sign and posted hours of operation.

- **Standard 9:** Maintain a primary business telephone listed under the name of the business locally or toll-free for beneficiaries.

- **Standard 10:** Have a comprehensive liability insurance policy in the amount of at least $300,000 that covers both the supplier's place of business and all customers and employees of the supplier. Failure to maintain required insurance at all times will result in revocation of the supplier's billing privileges retroactive to the date the insurance lapsed.

- **Standard 14:** Must maintain and replace at no charge or repair directly, or through a service contract with another company, Medicare-covered items it has rented to beneficiaries. The item must function as required and intended after being repaired or replaced.

NSC verifies compliance with the 25 standards, primarily during enrollment and reenrollment, through on-site inspections conducted by subcontractors, and desk reviews conducted by NSC analysts. NSC requires that site inspectors arrive unannounced for any inspection. Before the inspection, NSC provides the inspectors with briefing information on the supplier, including information on whether the supplier is enrolling or reenrolling and the type of state licenses to verify. While on site, inspectors are expected to take photographs of the supplier's sign with its business name, posted hours of operation, complete inventory in stock, and facility. NSC also expects site inspectors to obtain copies of relevant documents, such as state licenses, comprehensive liability insurance policies, contracts with companies for inventory, and contracts for the service and maintenance of DMEPOS supplies. NSC analysts are expected to check that the supplier has all the state licenses that it would need to provide the items it disclosed in its application. The NSC analyst is also expected to contact the insurance underwriter to ensure that the supplier's policy is valid and the post office to make sure the supplier's address is listed. NSC also has a procedure to match data from its supplier database with computerized lists maintained by the federal government to ensure that supply company owners are not prohibited from participating in federal health care programs or debarred from federal contracting.

In addition, suppliers submitting an enrollment application to NSC on or after March 1, 2008, must also be accredited by an approved organization

prior to submitting the application. These accrediting organizations are supposed to ensure that prospective DMEPOS suppliers meet quality standards related to financial and human resource management, consumer management, product safety, product delivery, and beneficiary training, among others.[5] DMEPOS suppliers that enrolled for the first time between January 1, 2008, and February 29, 2008, must obtain accreditation by January 1, 2009. Suppliers that enrolled with Medicare before January 1. 2008, must obtain accreditation by September 30, 2009. Further, CMS is beginning to implement competitive bidding, which will change how suppliers obtain the right to participate in the program. Competitive 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. Competitive bidding provides CMS with the authority to select suppliers by screening their financial documents such as income statements and credit reports and other application materials. CMS has chosen suppliers to serve beneficiaries in 10 Metropolitan Statistical Areas and the program is scheduled to begin July 1, 2008.

Apart from the competitive bidding program, as long as suppliers can demonstrate that they comply with all the standards and have not been excluded from participating in any federal health care program, NSC must enroll or reenroll them in Medicare. Enrolled suppliers are issued a Medicare billing number. If NSC discovers that a new applicant or enrolled supplier is not in compliance with any of the 25 standards, NSC can deny the application or, with CMS's approval, revoke the supplier's billing number.[6] Suppliers whose applications have been denied or whose numbers have been revoked can submit a plan to NSC to correct the noncompliance, appeal the denial or revocation by requesting a hearing or both.

In January 2008, CMS proposed creating five new standards and strengthening several of the existing standards.[7] The new standards

[5]The quality standards are available at http://www.cms.hhs.gov/MedicareProviderSupEnroll/.

[6]First-time applicants for enrollment can be denied, while DMEPOS suppliers currently enrolled in the program that are renewing their applications for billing privileges may have their current billing numbers revoked. DMEPOS suppliers must renew their Medicare enrollment application every 3 years.

[7]73 *Fed. Reg.* 4503 (Jan. 25, 2008).

require most suppliers to be open to the public for at least 30 hours per week and prohibit them from sharing an office with another supplier. They will also be required to maintain ordering and referring documentation received from physicians for 7 years. Finally, suppliers that have a federal or state tax delinquency will be prohibited from obtaining or retaining billing privileges. With regard to strengthening the existing standards, CMS will, among other things, require that suppliers maintain an office to store business records and will limit the use of cell phones, beeper numbers, pagers, and answering services as the primary DMEPOS business telephone number during posted hours of operation.

Testing the Medicare Enrollment Process

After establishing two fictitious DMEPOS storefronts with no inventory and no clients, our undercover investigators were able to successfully complete the Medicare enrollment process. Although CMS and NSC initially requested corrections to our paperwork and then denied our applications because we failed to comply with 2 of the 25 standards, they never detected the fact that our companies were fictitious. After submitting corrective action plans addressing the standards we failed, both companies were approved for Medicare billing privileges and provided with billing numbers. These numbers, in conjunction with billing passwords and software, allowed us to successfully complete Medicare's test billing process for our Virginia office. Based on a review of case studies we obtained from HHS IG, we believe that, had our operation continued successfully, we could have fraudulently billed Medicare for substantial sums—potentially reaching millions of dollars.

Creating Fictitious DMEPOS Companies

Prior to submitting applications to CMS to become approved DMEPOS suppliers, investigators easily set up two fictitious durable medical equipment companies during April and May 2007 using undercover names and bank accounts. Although we did not actually obtain any inventory, we decided that both companies would be generic medical supply companies, providing, among other things, commodes, diabetic supplies, surgical dressings, urinals and bedpans, walkers and canes, and manual wheelchairs. To appear legitimate, we rented 100 square foot commercial offices in both Maryland and Virginia. Both rentals cost approximately $1,000 per month and came complete with Internet, phone and fax service, and a shared secretary. We also set up fictitious Web sites, created brochures and business cards, and purchased a few "props" to be prepared for on-site inspections, including a wheelchair and bed pan.

Our investigators for the most part followed the general procedures that any legitimate business would use to begin DMEPOS operations. First, they paid online registration companies about $400 per supplier to obtain required state business licenses, such as sales tax licenses. In addition, for each company, investigators obtained employer identification numbers (EIN) from the Internal Revenue Service (IRS) and National Provider Identification (NPI) numbers from CMS.[8] Investigators obtained both numbers for free online using basic information, such as the business name and address.

To make sure that our companies would meet the requirements for DMEPOS suppliers as outlined in the 25 standards, we did the following.

- We created phony contracts with two fictitious DMEPOS wholesale suppliers to demonstrate that we had the capacity to supply equipment and supplies to clients. We also established phone numbers for each fictitious wholesale supplier. In reality, these phone numbers were unmanned extensions in the GAO building.

- We created signs for the office doors listing hours of operations and staffed the offices with undercover agents posing as sales representatives.

- We purchased approximately $3 million worth of general liability insurance covering, among other things, property damage and employee injury, at a cost of $550 annually.

[8]An EIN is issued to any person or company who must pay withholding taxes on employees, while an NPI is a unique identification number for covered health care providers and is required to enroll in Medicare.

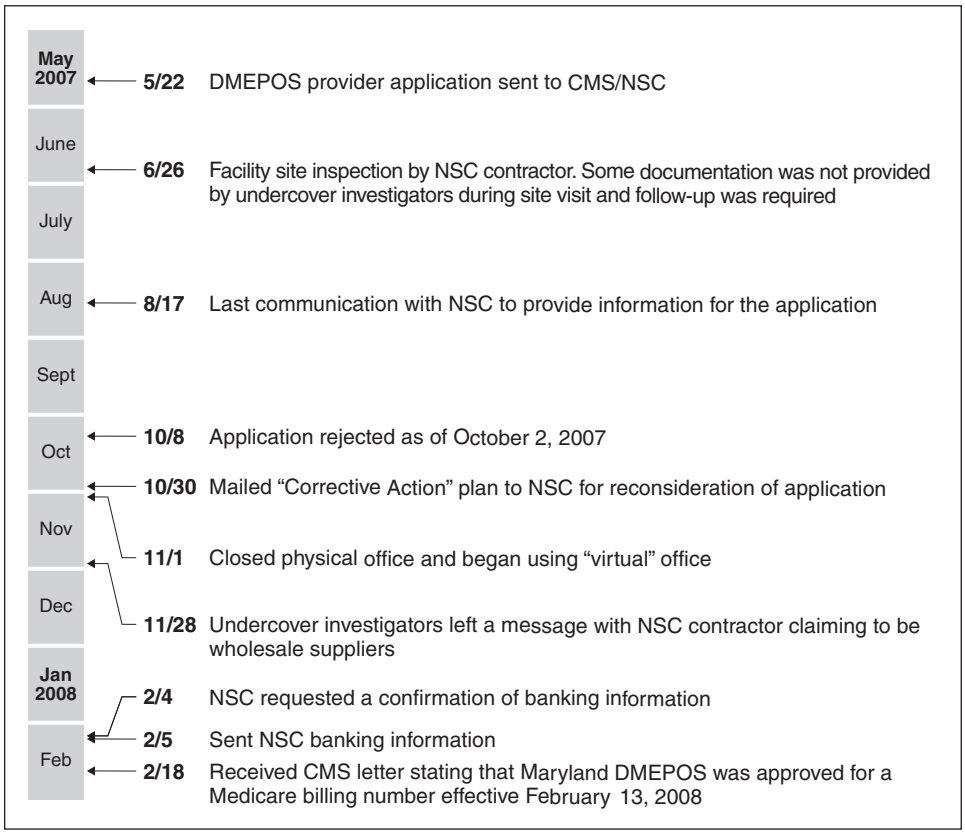
Obtaining a Medicare Billing Number

The approval process for both applications[9] was similar and the site inspections were even conducted by the same individual, who identified several discrepancies related to our office paperwork. Even though we corrected these discrepancies and submitted all required documentation, both of our applications were initially denied due to lack of compliance with two of the standards. In particular, even though we had already submitted our contracts with phony wholesale suppliers, CMS said that we did not demonstrate that we had the capacity to fill orders for equipment or supplies using our own inventory or by contracting with other companies, as per Standard 4. According to CMS, we also did not demonstrate that we could replace or repair the items we provided to beneficiaries, as per Standard 14. To comply with these two standards, we sent NSC corrective action plans that included repair policies and the same phony DMEPOS wholesale supplier contracts that we had previously submitted. CMS accepted this documentation as valid and approved both of our fictitious DMEPOS companies. In short, the subcontractors hired to review our applications ultimately focused on the technical and administrative completeness of our applications rather than attempting to determine whether we were running valid businesses.

Maryland Application Review and Site Visits: The application review process for our fictitious Maryland DMEPOS company took approximately 9 months, from the end of May 2007 until February 2008, when we received an approval letter from CMS containing a Medicare billing number. As shown in figure 1 and described in the following narrative, although NSC and its subcontractors identified several administrative discrepancies, they never uncovered the fact that our DMEPOS company was a fraudulent business.

[9]The Medicare enrollment application was straightforward and easy to complete. In addition to supplying our business names, locations, mailing addresses, and phone numbers, we also had to state what type of supplier we were applying to be (e.g., an ambulatory surgical center; a nursing care facility; an oxygen supplier; or a medical supply company) and what type of products we were going to supply. We were also asked to provide information regarding any previous legal actions taken against our companies and their owners. Finally, we had to certify that we had made no false statements on the applications and that we would not knowingly present a fraudulent claim for payment. We were also asked to submit copies of all federal and state licenses, our liability insurance, and forms authorizing electronic funds transfer.

Figure 1: Timeline of Maryland DMEPOS Supplier Application and Approval Process



Source: GAO.

As shown in the figure, we sent our application for review on May 22, 2007. On June 26, 2007, a representative from a contractor hired by NSC to conduct inspections visited the office. The representative explained to our undercover investigator, who was posing as a salesperson, that the visit would be used to gather information needed to verify compliance with CMS's standards. Using a checklist, the representative asked questions about the company's return policy, how the items were going to be delivered, and whether we had a warehouse or if we would have items drop-shipped from a supplier. He also asked if any member of our fictitious owner's family was in the medical supply business, if the owner had any business partners, and if there were any investors. The representative also asked for copies of our state licenses, insurance policy, and other documentation. Our investigator was deliberately vague in his responses to the representative and did not provide the inspector with any

of the requested documentation, telling the representative that the "owner" had all that information.

The representative also took pictures of the office to make sure that the building was accessible to persons with disabilities. He asked for our insurance documentation and noted that it was missing the company's physical address. Finally, he mentioned that the business needed a sign in the office window identifying its location and hours. We did not have the hours posted because the building where our office was located had a policy prohibiting postings on office windows; however, the investigator told the representative that he would speak to the building managers and ensure that the hours were posted. The representative then presented our investigator with a site visit acknowledgement form and checked off the following eight documents that needed to be provided to NSC as required by the standards:

- required licenses, including zoning,
- complaint log,
- complaint resolution protocol,
- rental/purchase option agreement,
- comprehensive liability insurance,
- credit agreements or invoices,
- proof of warranty coverage, and
- written instructions on beneficiary use.

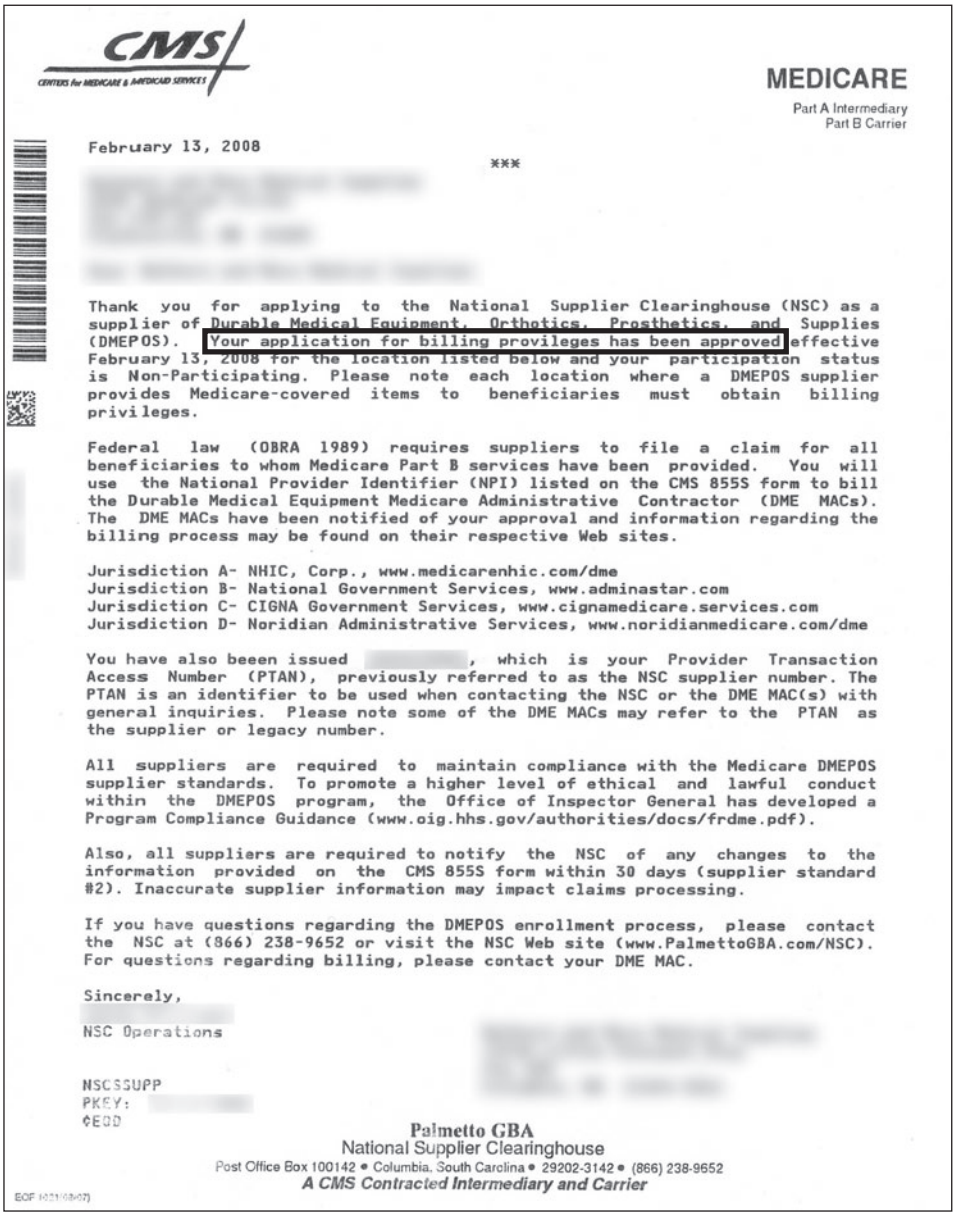
One day later, we sent NSC the information requested on the checklist. On July 17, 2007, NSC requested a full copy of the over 100 page insurance policy; we had sent an abbreviated version provided by our carrier after the site visit, but NSC wanted a complete copy. We immediately contacted the carrier and they agreed to send a complete copy directly to NSC. On August 15, 2007, NSC requested that we provide it with warranty information for DMEPOS rentals and we faxed the information on August 17. We had no further communication with NSC or the subcontractor who conducted the site visit until we called on October 3, 2007, requesting information about the status of our application.

On October 8, we received a letter from CMS denying our application for a billing number because our company did not adhere to 2 of the 25 standards. Specifically, even though we had already submitted our contracts with phony wholesale suppliers, CMS said that we did not demonstrate that we had the capacity to fill orders for equipment or supplies using our own inventory or by contracting with other companies, as per Standard 4. According to the letter, we also did not demonstrate

that we could replace or repair the items we provided to beneficiaries, as per Standard 14. The letter also informed us that we could reopen our application by submitting a "corrective action plan" addressing our deficiencies within 90 days. As part of the corrective action plan, we sent NSC a repair policy and resubmitted our phony supplier contract on October 30, 2007. We also provided the contact numbers that we created for the wholesale suppliers and informed NSC that we had hired a full-time employee to take care of repair issues. On November 1, 2007, we closed down our physical office and switched to a "virtual office" in the same building, meaning that we no longer had designated office space but still had access to mail and fax services, the shared secretary, and meeting rooms.

Although we were never questioned about our plan to correct our repair policy, NSC did call the undercover phone number we set up for our phony DMEPOS wholesale supplier in November and left a message requesting additional information. Posing as a representative for this wholesale supplier, an undercover investigator left a vague message in response but did not confirm the existence of a contract or a credit line. NSC never returned these calls or conducted any other followup. Over the next several months, we repeatedly called NSC and its subcontractors to determine the status of our application and corrective action plan. Each time, we were told that our application was still under review. Finally, on February 4, 2008, NSC requested a voided check or deposit slip to confirm our banking information so that we could be set up for electronic funds transfers. We provided the information the next day, and CMS approved our application and sent us a Medicare billing number in its approval letter dated February 13, 2008 (see fig. 2).

Figure 2: Maryland DMEPOS Supplier Approval Letter



CMS
CENTERS for MEDICARE & MEDICAID SERVICES

MEDICARE
Part A Intermediary
Part B Carrier

February 13, 2008

***

[redacted]

Thank you for applying to the National Supplier Clearinghouse (NSC) as a supplier of Durable Medical Equipment, Orthotics, Prosthetics, and Supplies (DMEPOS). Your application for billing provileges has been approved effective February 13, 2008 for the location listed below and your participation status is Non-Participating. Please note each location where a DMEPOS supplier provides Medicare-covered items to beneficiaries must obtain billing privileges.

Federal law (OBRA 1989) requires suppliers to file a claim for all beneficiaries to whom Medicare Part B services have been provided. You will use the National Provider Identifier (NPI) listed on the CMS 855S form to bill the Durable Medical Equipment Medicare Administrative Contractor (DME MACs). The DME MACs have been notified of your approval and information regarding the billing process may be found on their respective Web sites.

Jurisdiction A- NHIC, Corp., www.medicarenhic.com/dme
Jurisdiction B- National Government Services, www.adminastar.com
Jurisdiction C- CIGNA Government Services, www.cignamedicare.services.com
Jurisdiction D- Noridian Administrative Services, www.noridianmedicare.com/dme

You have also beeen issued [redacted], which is your Provider Transaction Access Number (PTAN), previously referred to as the NSC supplier number. The PTAN is an identifier to be used when contacting the NSC or the DME MAC(s) with general inquiries. Please note some of the DME MACs may refer to the PTAN as the supplier or legacy number.

All suppliers are required to maintain compliance with the Medicare DMEPOS supplier standards. To promote a higher level of ethical and lawful conduct within the DMEPOS program, the Office of Inspector General has developed a Program Compliance Guidance (www.oig.hhs.gov/authorities/docs/frdme.pdf).

Also, all suppliers are required to notify the NSC of any changes to the information provided on the CMS 855S form within 30 days (supplier standard #2). Inaccurate supplier information may impact claims processing.

If you have questions regarding the DMEPOS enrollment process, please contact the NSC at (866) 238-9652 or visit the NSC Web site (www.PalmettoGBA.com/NSC). For questions regarding billing, please contact your DME MAC.

Sincerely,

[redacted]
NSC Operations

NSCSSUPP
PKEY: [redacted]
ΦEOD

Palmetto GBA
National Supplier Clearinghouse
Post Office Box 100142 • Columbia, South Carolina • 29202-3142 • (866) 238-9652
A CMS Contracted Intermediary and Carrier

EOF

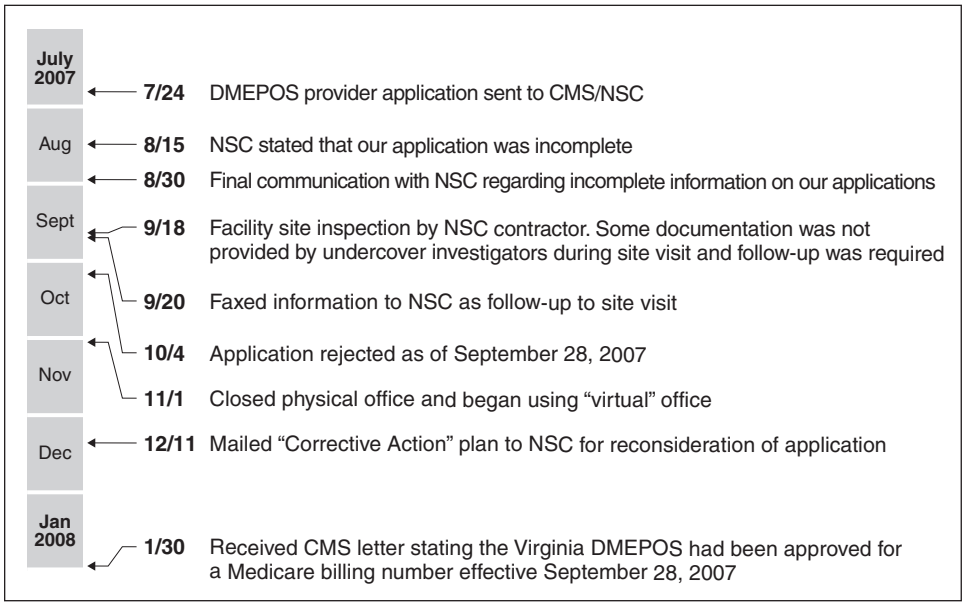
"Your application for billing privileges has been approved..."

Source: CMS.

Virginia Application Review and Site Visit: The application review process for our fictitious Virginia DMEPOS company took approximately 6

months, from the end of July 2007 until January 2008, when we received an approval letter retroactive to September 28, 2007, and a Medicare billing number. As shown in figure 3 and the following narrative, NSC's inspectors identified several discrepancies in our application and at our office but never uncovered the fact that our DMEPOS company was a fraudulent business.

Figure 3: Timeline of Virginia DMEPOS Supplier Application and Approval Process



Source: GAO.

As shown in figure 3, we sent our application for review on July 24, 2007. Although we complied with most of the application instructions, we did make several errors on the application. Specifically, we failed to provide copies of certain state licenses and certifications and did not check either "yes" or "no" when asked if we had any previous legal actions filed against the company or its owners. NSC detected these errors and on August 15, 2007, we received a letter stating that our application was incomplete. In addition, NSC requested clarification about our office location and requested a voided check or deposit slip to confirm our bank account so that we could be set up for electronic funds transfers. We corrected all these discrepancies by August 30, 2007.

NSC's representative, the same individual who inspected our Maryland office, inspected the site on September 18, 2007. As with the Maryland

office, this individual used a simple checklist to conduct the inspection and asked for the same documentation, including licenses, insurance policy, complaint protocols, rental agreement, and instructions for beneficiary use of the supplies. This time, the undercover investigator immediately provided almost all the information requested. The representative provided a site acknowledgment form with just one missing item checked off: written instructions on beneficiary use/maintenance of supplies. We sent these instructions to NSC on September 20, 2007.

On October 4, 2007, we received a letter from CMS denying our application for a billing number because our company did not adhere to 2 of the 25 standards—the same standards we had failed to comply with in Maryland. Specifically, we did not demonstrate that we had the capacity to fill orders for equipment or supplies using our own inventory or by contracting with other companies, as per Standard 4. According to the letter, we also did not demonstrate that we could replace or repair the items we provided to beneficiaries, as per Standard 14. As in Maryland, we sent NSC our repair policy and resubmitted our phony wholesale supplier contract on December 11, 2007, as part of our corrective action plan to show compliance with the standards.[10] Because our corrective action plans for the Maryland and Virginia offices were identical, we intentionally delayed sending our Virginia plan by several months so as not to arouse suspicion with NSC. We also provided the contact numbers that we created for the wholesale suppliers and informed NSC that we hired a full-time employee to take care of repair issues.

To our knowledge, NSC did not do any further investigation and accepted the existence of the fictitious DMEPOS wholesale suppliers we created. On January 30, 2008, we received an approval letter and Medicare billing number. The letter stated that the effective date of the approval was retroactive to September 28, 2007—the date our application was initially denied.

Completing Electronic Test Billing

After requesting an electronic billing enrollment package and obtaining passwords from CMS, we were able to successfully complete Medicare's often confusing test billing process for our Virginia office; we did not complete test billing for our Maryland office because we did not receive

[10]Prior to this date, on November 1, 2007, we closed down our physical office and switched to a "virtual office" in the same building.

the necessary passwords from CMS by the close of our investigation in June 2008. Had we been real fraudsters, we could have fraudulently billed Medicare for substantial sums, potentially reaching millions of dollars.

Although the Medicare approval letters we received contained billing numbers, they contained no instructions for how to begin the electronic billing process. Consequently, we had to do our own research on CMS and NSC Web sites in order to figure out that we needed to download billing enrollment packets so that we could be approved to submit electronic claims. We sent completed enrollment packets for both companies to CMS's contractor by the beginning of March 2008. These packets included billing applications, completed Electronic Data Interchange (EDI) agreements and software order forms, contact information, NPIs, and EINs for our two companies. We did not receive any further information related to the Maryland DMEPOS company. On March 13, 2008, we received, among other things, an electronic billing submitter identification number and password for the Virginia office. There were no instructions accompanying this information and it was not clear to which systems each applied.

Using billing software downloaded from the Web, we began processing claims by entering fictitious dates of service, our undercover beneficiary information, DMEPOS item codes and charges, generic diagnosis codes, our billing numbers, and physician identification numbers that we found on the Internet.[11] It is important to note that we only used the latter to complete test billing; we did not compromise the provider status of any legitimate physicians by submitting fraudulent claims using their identification information. We then submitted several completed claims to CMS for acceptance, but our first few attempts were rejected. Our undercover investigator called CMS's help desk for assistance and found that we had to input our billing number on one of CMS's billing-related Web sites.[12] There had been no instructions in the billing packet indicating that this was a required step. Once we provided our billing number at the site, CMS approved our initial claims. As required by the electronic enrollment application, DMEPOS suppliers must submit a single test file

[11]As specified by the billing software, we first created a series of "reference files" containing all this information to facilitate processing.

[12]When our claims were rejected, we received an error message which stated "NPI Not on Crosswalk." The help desk told us that we had to include our Virginia Medicare billing number in our NPI file on the National Plan and Provider Enumeration System Web site (NPPES) for our claims to be accepted.

with at least 25 claims that are 95 percent error-free in order to complete test billing. On May 14, 2008, we successfully submitted a file with 27 claims for $6,876.34 with no errors.

Case Studies Provide Real Examples of Fraudulent DMEPOS Suppliers

As shown by four closed cases from South Florida that we obtained from the HHS IG, criminals use similar techniques to establish fictitious DMEPOS suppliers and then employ billing schemes to obtain millions of dollars in Medicare funds from the government. Specifically, once criminals have created fraudulent DMEPOS companies, they typically steal or buy Medicare beneficiary numbers and physician identification numbers in order to repeatedly submit claims.

Case Study 1: The owner of this fraudulent company admitted to HHS that she started her DMEPOS company after working as a secretary for another fraudulent company. She rented an office in the same location as this company and worked with her former employer to obtain all the required state licenses. She also purchased fake invoices for DMEPOS equipment from another company to make it seem as though she was obtaining legitimate supplies from a wholesaler. In February 2005, she received her Medicare provider number and then provided her former employer with kickbacks in order to have access to Medicare beneficiary numbers. From January 1, 2006, through April 30, 2007, she submitted about $1.5 million in claims to Medicare for supplies including urinary bags, tubing, canisters, and air mattresses. Ultimately, Medicare paid the company $372,286. The owner was indicted for health care fraud on September 11, 2007, and was convicted and sentenced on January 22, 2008, to 30 months imprisonment and 3 years supervised release, and ordered to pay $372,286 in restitution.

Case Study 2: This case relates to three fraudulent companies with the same owner. In October 2006, the owner bought a DMEPOS company that had been incorporated in August 2006 and used the original owner's identity, billing number, and beneficiaries to submit claims in an attempt to avoid detection by CMS. The new company used an address in Coral Gables but did not have a real office and did not serve customers. The owner also stole the personal identification numbers of licensed physicians. According to the HHS IG, these physicians did not have any involvement with the company and did not provide care or prescriptions related to the submitted claims. During the course of its investigation, HHS discovered that the owner had opened another fraudulent DMEPOS company. This company used a utility closet as its address—HHS investigators found buckets of sand mix, road tar, and a large wrench in the room, but no medical files, office equipment, or telephone. This time,

the owner used a fictitious physician name and identification number to submit claims to CMS; CMS confirmed that this number should not have passed the initial computer system edit for payment. Finally, while conducting a financial analysis of the second company's bank account records, investigators found that the owner operated yet another fraudulent DMEPOS company. In total, from October 2006 through March 2007, the owner submitted claims from these three companies in excess of $5.5 million and ultimately received about $77,000 from Medicare. In August 2007, the owner was sentenced to 37 months in prison for conspiracy to commit health care fraud, ordered to pay over $70,000 in restitution, and made to forfeit his Miami home and Rolls Royce.

Case Study 3: This company billed Medicare for $4.4 million dollars worth of supplies and services that were never delivered. These claims were submitted between March and July 2006 using real beneficiary numbers that the DMEPOS company owner had purchased illegally. Ultimately, Medicare paid approximately half of these claims ($2.2 million). According to HHS IG records, the only employee not involved in the scheme was a secretary who told investigators that there was never any business activity in the office and that the owner rarely visited. She also stated that Medicare beneficiaries often called her to complain that they had received an explanation of benefits letter in the mail even though they did not receive any supplies or services. The Bank of America eventually filed a suspicious activity report as a result of the company's billing practices. The Federal Bureau of Investigation (FBI) and HHS IG subsequently determined that the owner stole the identities and physician identification numbers of practicing physicians to legitimize his fraudulent claims. The owner plead guilty to one count of health care fraud and on March 16, 2007, was sentenced to 4 years in prison and 3 years of probation, assessed a $100 fee, and ordered to pay $2.2 million in restitution.

Case Study 4: The owner of this DMEPOS company operated a fictitious supply business out of an office connected to a real estate company and purchased real Medicare beneficiary numbers illegally for $45 each in order to submit claims. Through data mining, the HHS IG determined that the company displayed billing patterns that were highly consistent with known fraudulent practices. Specifically, the company owner used a small number of stolen physician identification numbers to submit numerous claims for expensive DMEPOS items that are typically used in fraudulent schemes, including motorized wheelchairs, wound therapy pumps, and infusion equipment. From July 2005 through October 2006, the DMEPOS company billed the Medicare program over $1 million and received over

$500,000 in payments. On August 7, 2007, the owner was ordered to pay $702,186 in restitution to Medicare and was sentenced to 2 years in federal prison and 3 years of probation.

Corrective Action Briefing

On June 18, 2008, we informed representatives from CMS about the results of our investigation. In response, they stated that they are implementing new supplier requirements, including the accreditation process and the revisions and additions to the 25 standards that were proposed in January 2008. They also acknowledged that our covert testing illustrates gaps in oversight that still require improvement and stated that they would continue to work to strengthen the entire DMEPOS enrollment process.

Conclusion

Although CMS took actions to address our prior recommendations, we found that the fraud prevention controls in place during our investigation were not effective in preventing our fictitious DMEPOS companies from obtaining legitimate Medicare billing numbers and completing test billing. As indicated, CMS is currently taking additional actions to strengthen both the 25 standards and its oversight of the DMEPOS supplier enrollment process; however, these actions will only be successful if those tasked with ensuring compliance exercise due diligence when conducting screenings and inspections. Our covert tests clearly demonstrate that a simple paperwork review is not sufficient. Unless CMS and its contractors scrutinize suppliers to ensure that they are responsible, legitimate businesses, DMEPOS fraud will continue to cost taxpayers billions of dollars each year.

As agreed with your offices, unless you announce the contents of this report earlier, we will not distribute it until 30 days from its date. At that time, we will send copies to the Administrator of CMS and other interested parties. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

Please contact me at (202) 512-6722 or kutzg@gao.gov if you have any questions concerning this report. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. Key contributors are listed in appendix II.

Gregory D. Kutz
Managing Director
Forensic Audits and Special Investigations

Appendix I: 25 Standards for Medicare Suppliers of Durable Medical Equipment, Prosthetics, Orthotics, and Supplies

Standard number	Description of what a supplier must do
1	Operates its business and furnishes Medicare-covered items in compliance with all applicable Federal and State licensure and regulatory requirements.
2	Has not made, or caused to be made, any false statement or misrepresentation of a material fact on its application for billing privileges. (The supplier must provide complete and accurate information in response to questions on its application for billing privileges. The supplier must report to CMS any changes in information supplied on the application within 30 days of the change.)
3	Must have the application for billing privileges signed by an individual whose signature binds a supplier.
4	Fills orders, fabricates, or fits items from its own inventory or by contracting with other companies for the purchase of items necessary to fill the order. If it does, it must provide, upon request, copies of contracts or other documentation showing compliance with this standard. A supplier may not contract with any entity that is currently excluded from the Medicare program, any State health care programs, or from any other Federal Government Executive Branch procurement or nonprocurement program or activity.
5	Advises beneficiaries that they may either rent or purchase inexpensive or routinely purchased durable medical equipment, and of the purchase option for capped rental durable medical equipment, as defined in § 414.220(a) of this subchapter. (The supplier must provide, upon request, documentation that it has provided beneficiaries with this information, in the form of copies of letters, logs, or signed notices.)
6	Honors all warranties expressed and implied under applicable State law. A supplier must not charge the beneficiary or the Medicare program for the repair or replacement of Medicare covered items or for services covered under warranty. This standard applies to all purchased and rented items, including capped rental items, as described in § 414.229 of this subchapter. The supplier must provide, upon request, documentation that it has provided beneficiaries with information about Medicare covered items covered under warranty, in the form of copies of letters, logs, or signed notices.
7	Maintains a physical facility on an appropriate site. The physical facility must contain space for storing business records including the supplier's delivery, maintenance, and beneficiary communication records. For purposes of this standard, a post office box or commercial mailbox is not considered a physical facility. In the case of a multi-site supplier, records may be maintained at a centralized location.
8	Permits CMS, or its agents to conduct on-site inspections to ascertain supplier compliance with the requirements of this section. The supplier location must be accessible during reasonable business hours to beneficiaries and to CMS, and must maintain a visible sign and posted hours of operation.
9	Maintains a primary business telephone listed under the name of the business locally or toll-free for beneficiaries. The supplier must furnish information to beneficiaries at the time of delivery of items on how the beneficiary can contact the supplier by telephone. The exclusive use of a beeper number, answering service, pager, facsimile machine, car phone, or an answering machine may not be used as the primary business telephone for purposes of this regulation.
10	Has a comprehensive liability insurance policy in the amount of at least $300,000 that covers both the supplier's place of business and all customers and employees of the supplier. In the case of a supplier that manufactures its own items, this insurance must also cover product liability and completed operations. Failure to maintain required insurance at all times will result in revocation of the supplier's billing privileges retroactive to the date the insurance lapsed.

Standard number	Description of what a supplier must do
11	Must agree not to contact a beneficiary by telephone when supplying a Medicare-covered item unless one of the following applies: (i) The individual has given written permission to the supplier to contact them by telephone concerning the furnishing of a Medicare-covered item that is to be rented or purchased. (ii) The supplier has furnished a Medicare-covered item to the individual and the supplier is contacting the individual to coordinate the delivery of the item. (iii) If the contact concerns the furnishing of a Medicare-covered item other than a covered item already furnished to the individual, the supplier has furnished at least one covered item to the individual during the 15-month period preceding the date on which the supplier makes such contact.
12	Must be responsible for the delivery of Medicare covered items to beneficiaries and maintain proof of delivery. (The supplier must document that it or another qualified party has at an appropriate time, provided beneficiaries with necessary information and instructions on how to use Medicare-covered items safely and effectively.)
13	Must answer questions and respond to complaints a beneficiary has about the Medicare-covered item that was sold or rented. A supplier must refer beneficiaries with Medicare questions to the appropriate carrier. A supplier must maintain documentation of contacts with beneficiaries regarding complaints or questions.
14	Must maintain and replace at no charge or repair directly, or through a service contract with another company, Medicare-covered items it has rented to beneficiaries. The item must function as required and intended after being repaired or replaced.
15	Must accept returns from beneficiaries of substandard (less than full quality for the particular item) or unsuitable items (inappropriate for the beneficiary at the time it was fitted and rented or sold) from beneficiaries.
16	Must disclose these supplier standards to each beneficiary to whom it supplies a Medicare-covered item.
17	Must comply with the disclosure provisions in § 420.206 of this subchapter.
18	Must not convey or reassign a supplier number.
19	Must have a complaint resolution protocol to address beneficiary complaints that relate to supplier standards in paragraph (c) of this section and keep written complaints, related correspondence and any notes of actions taken in response to written and oral complaints. Failure to maintain such information may be considered evidence that supplier standards have not been met. (This information must be kept at its physical facility and made available to CMS, upon request.)
20	Must maintain the following information on all written and oral beneficiary complaints, including telephone complaints, it receives: (i) The name, address, telephone number, and health insurance claim number of the beneficiary. (ii) A summary of the complaint; the date it was received; the name of the person receiving the complaint, and a summary of actions taken to resolve the complaint. (iii) If an investigation was not conducted, the name of the person making the decision and the reason for the decision.
21	Provides to CMS, upon request, any information required by the Medicare statute and implementing regulations.
22	All suppliers of DMEPOS and other items and services must be accredited by a CMS-approved accreditation organization in order to receive and retain a supplier billing number. The accreditation must indicate the specific products and services, for which the supplier is accredited, in order for the supplier to receive payment for those specific products and services.
23	All DMEPOS suppliers must notify their accreditation organization when a new DMEPOS location is opened. The accreditation organization may accredit the new supplier location for three months after it is operational without requiring a new site visit.

Standard number	Description of what a supplier must do
24	All DMEPOS supplier locations, whether owned or subcontracted, must meet the DMEPOS quality standards and be separately accredited in order to bill Medicare. An accredited supplier may be denied enrollment or their enrollment may be revoked, if CMS determines that they are not in compliance with the DMEPOS quality standards.
25	All DMEPOS suppliers must disclose upon enrollment all products and services, including the addition of new product lines for which they are seeking accreditation. If a new product line is added after enrollment, the DMEPOS supplier will be responsible for notifying the accrediting body of the new product so that the DMEPOS supplier can be re-surveyed and accredited for these new products.

Source: 42 C.F.R. § 424.57(c).

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

Gregory D. Kutz, (202) 512-6722 or kutzg@gao.gov

Staff Acknowledgments

In addition to the individual named above, Matthew Harris, Assistant Director; Erika Axelson; Gary Bianchi; Valerie Blyther; Norman Burrell; Ray Bush; Shafee Carnegie; Jennifer Costello; Paul Desaulniers; Dennis Fauber; Craig Fischer; Janice Friedeborn; Jessica Gray; Ken Hill; Christine Hodakievic; Jason Kelly; Barbara Lewis; Christopher Madar; Jeffrey McDermott; Andrew McIntosh; Keith Steck; and Viny Talwar made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, DC 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

Ralph Dawn, Managing Director, dawnr@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