United States General Accounting Office

GAO

Report to the Ranking Minority Member,
Subcommittee on Labor, Health and
Human Services, Education, and Related
Agencies, Committee on Appropriations,
U.S. Senate

August 1995

MEDICARE

Antifraud Technology Offers Significant Opportunity to Reduce Health Care Fraud

GAO/AIMD-95-77

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-260886

August 11, 1995

The Honorable Tom Harkin
Ranking Minority Member
Subcommittee on Labor, Health
and Human Services,
Education, and Related Agencies
Committee on Appropriations
United States Senate

Dear Senator Harkin:

This report responds to your September 1, 1994, request for information on existing tools used by the Medicare program to detect and prevent fraud, and discusses the availability of other technologies to assist in combatting fraudulent billing.[1] This evaluation focused on Medicare part B benefits, which cover physician, supplier, and other outpatient services, provided at a cost of about $60 billion during 1994. This portion of the Medicare program currently constitutes slightly over a third of total Medicare costs (part A—hospital care—makes up the rest) and is expected to become an increasingly larger share.

In addition, this report addresses your request for information on Medicare fraud being perpetrated in South Florida and actions being taken to mitigate this problem. It also complements our recently issued report on abusive Medicare billing practices and existing information technology to help avoid the payment of abusive claims.[2]

Currently, no reliable estimate of the cost of fraud to the Medicare program exists; however, health care experts have estimated that as much as 10 percent of national health care spending is attributable to waste, fraud, and abuse. Although the Department of Health and Human Service's (HHS) Health Care Financing Administration (HCFA), which manages the Medicare program, has acted to reduce program fraud, the program remains vulnerable in this area. Thus, we added the Medicare program to our list of high-risk government programs in 1992.[3]

[1] Abuse also involves actions resulting in inappropriate Medicare program costs. However, fraud differs from abuse in that it is an illegal act that involves obtaining something of value through willful misrepresentation.

[2] Medicare Claims: Commercial Technology Could Save Billions Lost to Billing Abuse (GAO/AIMD-95-135, May 5, 1995).

[3] Medicare Claims (GAO/HR-93-6, December 1992). This information has been updated in Medicare Claims (GAO/HR-95-8, February 1995).

HCFA contracts with 32 insurance companies, called carriers, who processed 623 million Medicare part B claims in 1994. These carriers are also responsible for protecting program funds by developing payment controls and performing other review activities called payment safeguards. Medicare fraud units within each carrier are the focal points for coordinating and referring potential fraud cases to the HHS Office of Inspector General (OIG).

Results in Brief

Medicare's controls against fraud have not kept pace with today's health care environment in which the number of claims processed—and those submitted electronically—have risen dramatically. Processed Medicare part B claims reached 623 million in 1994, a 32-percent jump in 4 years. The percentage processed electronically doubled during this period, from 36 to 72 percent. While electronic claims processing is critical for efficiency, when the volume rises to this degree, it also increases the need for more innovative controls to curtail fraud.

Existing Medicare carriers' controls rely on data from systems that may identify potential fraud, but were primarily designed for other purposes, such as identifying services that are not medically necessary or were overutilized. Medicare carrier fraud units also rely heavily on beneficiary complaints to identify discrepancies between services rendered and those billed. Each of these controls, however, have inherent limitations in detecting attempted fraud.

New antifraud systems are available and used today by private insurers, some of whom are also Medicare carriers. This technology may complement existing—and planned—Medicare systems. The principal advantage of these sophisticated systems is their ability to recognize patterns in paid claims data and thus identify potentially fraudulent relationships. While it is too early to fully document the cost-effectiveness of such systems, several potential fraud cases have been detected by this new technology, indicating that these systems can be cost-beneficial in combatting emerging types of fraud. Such technology may ultimately be utilized in the claims-processing environment to delay or even prevent the payment of questionable claims submitted by suspect providers.

Florida, with its highly publicized health care fraud issues, may be a logical place to start expanding Medicare's fraud detection capabilities with innovative and more imaginative approaches, and new antifraud technologies. Although Florida represents 7 percent of the Medicare beneficiary population, in fiscal year 1994, Florida accounted for over 20 percent of Medicare part B spending. In addition, reports continue to indicate that South Florida in particular has been victimized by new types of fraud—often by persons impersonating legitimate health care providers. In response to this problem, HCFA formed the interagency South Florida Workgroup, to coordinate enforcement actions, identify specific problems, and recommend corrective actions. This effort has identified several problems, including attempted fraud due to weaknesses in the provider enrollment process.

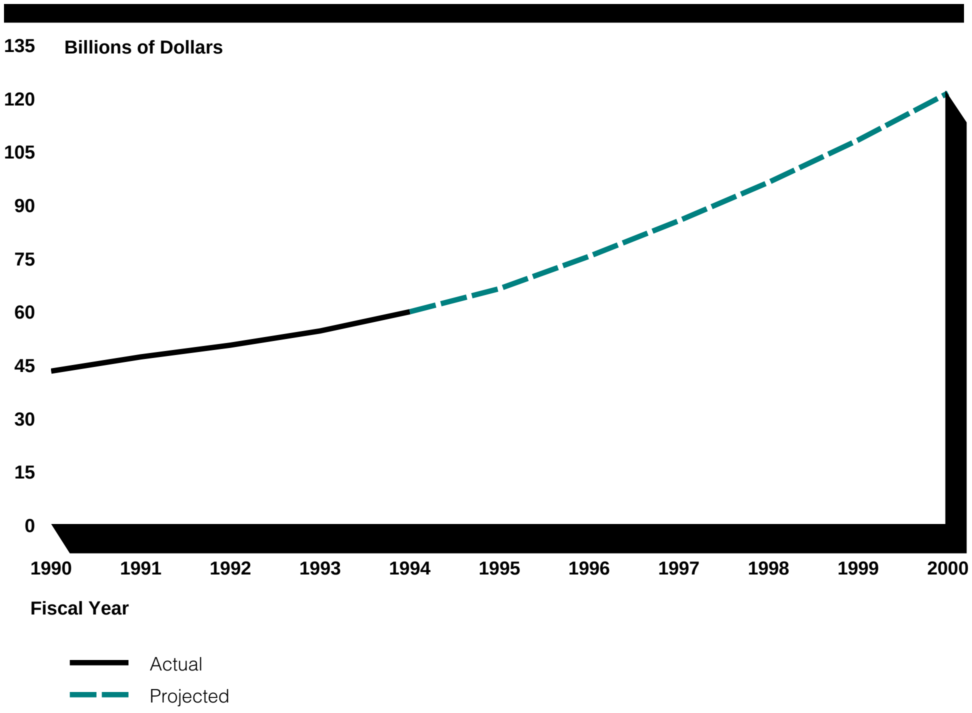
Background

Authorized in 1965 under title XVIII of the Social Security Act, Medicare pays for health care services and supplies for millions of beneficiaries,[4] mostly elderly, and provides direct payment to 1 million providers and suppliers of services. Medicare provides coverage under two sections: part A, primarily hospital insurance, and part B, supplementary insurance. Part B covers physician services, outpatient hospital care, medical supplies, and other health benefits, such as emergency ambulance services. Medicare part B generally pays 80 percent of the Medicare-approved amounts, with beneficiaries responsible for the remaining 20 percent (the copayment).

Medicare part B program costs (mainly direct payments to providers) rose an average of 9 percent per year from fiscal year 1990 through fiscal year 1994, increasing from $43 billion to $60 billion. These costs are expected to almost double over the next 5 years. Figure 1 depicts actual and projected increases in Medicare part B outlays from 1990 to 2000.

[4] Medicare insures 36 million people aged 65 and over, and individuals under 65 who are disabled.

Figure 1: Medicare Part B Outlays, 1990-2000



Note: We did not independently verify these figures.

Sources: Overview of Entitlement Programs, 1994 Green Book, Committee on Ways and Means, U.S. House of Representatives, 103rd Congress, 2nd Session, 1994; and Congressional Budget Office: The Economic and Budget Outlook, Fiscal Years 1996-2000, January 1995.

As part of their contract to process, review, and pay claims for covered services, Medicare carriers receive funding to perform payment safeguard activities. These activities are mainly performed by claims processing, medical review, and fraud units. Claims processing units ensure that Medicare claims are paid properly. These units also review claims that are suspended due to prepayment controls. Medical review units perform payment safeguard activities by identifying questionable billing patterns and practices. Potential fraud cases identified by either the claims processing or medical review units are referred to fraud units. Fraud units are responsible for examining these referrals, as well as tips and complaints received from beneficiaries, government agencies, or other sources, to determine their validity. Fraud units also forward potential fraud cases to the HHS OIG, as appropriate, for further investigation and possible punitive actions, such as fines, exclusion from the Medicare program, or referral to the Department of Justice for criminal or civil action.

Scope and Methodology

We reviewed HCFA's documentation on Medicare carrier antifraud responsibilities, functions, workload, and funding. We met with HCFA officials at HCFA's headquarters in Baltimore and at the Atlanta regional office. We also interviewed all 32 Medicare carrier fraud unit managers and met with several representatives from their claims processing and medical review units to learn how potential fraud is detected and what tools are being used to support this effort. We obtained views on health care antifraud activities by meeting with officials from the HHS OIG and the Department of Justice. Finally, we met with representatives of the private sector to obtain information on antifraud technology.

Our work was performed from August 1993 through May 1995, in accordance with generally accepted government auditing standards. Details of our scope and methodology are in appendix I. We requested written comments on a draft of this report from the Secretary of Health and Human Services or her designee. The Inspector General of the Department of Health and Human Services provided us with written comments. These comments are discussed in the Agency Comments and Our Evaluation section of the report and are reprinted in appendix II.

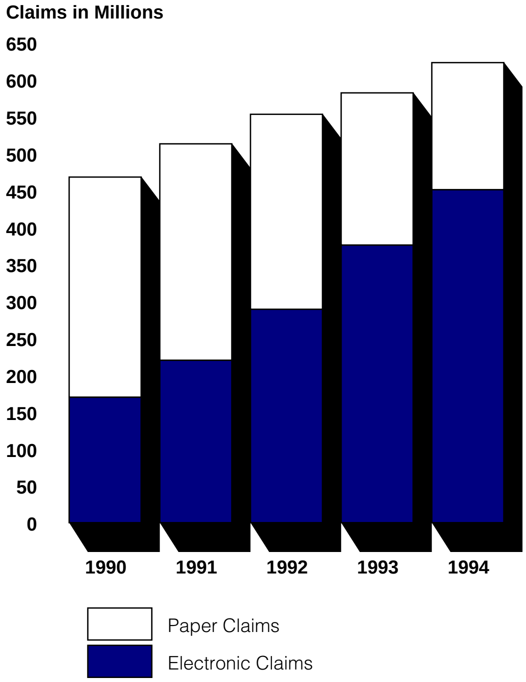
Existing Payment Safeguards Detect Fraud but Have Limitations

Over the past several years, HCFA has initiated a number of actions to increase the efficiency and effectiveness of its controls over fraud. Although these controls have been implemented within various functions throughout the 32 Medicare carriers, they have limitations that do not address the full spectrum of changes in today's health care environment.

Rapidly Changing Health Care Environment Makes Fraud Detection More Difficult

The already difficult task of detecting fraud has become a greater challenge as the number of Medicare part B claims has increased from 468 million in 1990 to 623 million in 1994. At the same time, the percentage of claims processed electronically doubled from 36 to 72 percent, with further increases likely. Figure 2 shows the volume of Medicare part B claims processed from paper and electronic submissions from 1990 through 1994.

Figure 2: Medicare Part B Claims Submitted on Paper and Electronically, 1990-1994



Source: HCFA.

The former Secretary of Health and Human Services initiated the Workgroup for Electronic Data Interchange in 1991 to reduce administrative costs in the nation's health care system by promoting electronic claims submission. HCFA promoted this initiative by requiring that carriers reimburse providers for electronic claims more quickly than for paper claims (14 days versus 27 days), thus encouraging providers to submit more claims electronically. This is an important gain, and the increased use of electronic claims submission should be encouraged; however, this method also increases the need for more innovative controls to curtail fraud.

With paper claims, signatures of providers and any obvious alterations to documents are apparent to claims adjudicators. In addition, the same types of claims (for example, by medical specialty) typically were handled by the same adjudicator. Therefore, aberrations could be more easily spotted. In contrast, electronic claims submission eliminates human intervention and thus any opportunity to examine provider signatures or detect any alterations to claims data.

Existing Medicare Electronic and Manual Controls Can Identify Potential Fraud

HCFA requires Medicare carriers to implement various manual and electronic fraud-detection controls, such as prepayment edits, medical review of overutilized and medically unnecessary procedures, and review of beneficiary complaints. Electronic controls within claims processing systems suspend claims with erroneous or incomplete data. These controls include, for example, edits to determine whether the number and accuracy of digits in a provider's billing number or beneficiary's identification number are correct. Such edits also check for duplicate claims, beneficiary eligibility, and whether the procedure cited in the claim was possible for the beneficiary's gender. Also, the system suspends claims that are flagged by electronic edits as not meeting certain conditions for payment. For example, if foot care is covered only under certain conditions, claims not meeting these conditions will be suspended until further review.

Medical review is another manual and electronic control that can serve to identify potential fraud. This function, which HCFA requires carriers to perform, primarily involves identifying abuse and overutilization, and preventing payments for medically unnecessary and noncovered services. According to HCFA data, in 1994, medical review referrals were among the 23,290 referrals made to carrier fraud units, and approximately 4,100 of these were subsequently referred to the HHS OIG.[5] Two kinds of postpayment medical review exist, with differing emphases. In the first type, called focused medical review, each of the 32 carriers examines national statistics to identify specific types of medical procedure codes for which the carrier exceeds the national Medicare norm. By changing individual carrier payment policies for such procedures and educating providers to bill correctly, HCFA hopes to discourage the submission of claims for noncovered or unnecessary services. In the second type, called comprehensive medical review, carriers audit individual providers whose claims appear to demonstrate a pattern of overutilizing procedures or performing those that are not medically necessary.

HCFA required carriers to obtain automated systems to support medical review functions and identify areas requiring special attention. These systems, for example, contain paid-claims data and use such techniques as

[5] HCFA combines potential fraud referrals from providers, medical review, and special requests from the OIG or HCFA into one category; therefore, we could not determine the number of referrals made specifically by medical review.

trend analysis to profile providers and identify those who bill disproportionately, causing a carrier to exceed the national Medicare utilization norm. These providers are then ranked for investigation, based on the extent to which they exceed specified limits, such as the number of services provided. Further investigation of these providers may identify cases of unnecessary medical care or overall aberrant practice patterns compared with peers within their specialty and locality. Based on the outcome of this investigation, the provider may be referred to the fraud unit as a potential fraud case. For instance, due to a comprehensive medical review, a provider identified for billing an excessive and, therefore, questionable amount of psychotherapy sessions on the same day was referred to the fraud unit because the carrier's psychiatric medical consultant determined that it would be impossible to perform that many procedures in 1 day.

Beneficiaries also serve as controls over fraud and abuse in the Medicare program and are considered to be the front-line defense for referring potential fraud cases to fraud units. Beneficiaries receive explanation of Medicare benefits (EOMB) statements that list charges submitted to Medicare and the amount paid to providers, thus uniquely positioning beneficiaries to identify payments for medical services or supplies that were not received or that they believe were unnecessary. HCFA encourages beneficiaries to notify carrier fraud units if they notice such discrepancies and requires carriers to analyze such complaints for their potential for fraud.

Medicare's Controls Have Technical and Funding Limitations

While HCFA has implemented Medicare part B controls that may identify fraud, these controls have technical limitations. In addition, per-claim funding for Medicare program safeguard activities declined by over 20 percent from 1989 through 1993.

Prepayment electronic edits help ensure that billed services are paid correctly, but these edits are not specifically designed to detect indicators of potential fraud. HCFA has progressively reduced the percentage of claims that can be suspended and reviewed by the carrier prior to payment from 20 percent during 1989 to 5 percent in 1994, due to per-claim reductions in safeguard funding.

Fraud-detection capabilities of medical review are limited since the systems used for this function usually concentrate on relatively few variables, such as the total number of services per beneficiary. These systems typically do not examine questionable behavior patterns, including the percentage of visits on Sundays and holidays, and a percentage of billing outside of the providers' geographic area. According to private industry, fraud is difficult to detect in this manner because individual billing patterns may not reveal anything meaningful about the overall behavior of a provider. In some cases, medical review systems results may be distorted when, for example, a cancer specialist is classified as an internist and measured against other internists on the number of laboratory tests rendered. Since cancer specialists perform a relatively high number of laboratory tests, misclassified internists would appear to have significantly exceeded the normal rates for laboratory tests when compared to all internists.

One medical review unit manager stated that another difficulty in detecting fraud through medical review systems is the risk that the data from which they evaluate trends may be skewed if the peer group as a whole is engaging in egregious billing patterns. Also, as long as fraud perpetrators stay within the parameters of payment policies and peer group norms, they may escape detection. Funding limitations have also constrained medical review, with HCFA reducing the number of providers audited from 8 per 1,000 providers in 1992 to 3 per 1,000 in 1995.

As post-payment safeguards, beneficiary complaints are only effective if recipients receive an EOMB statement and conscientiously report apparent discrepancies. For example, numerous cases have been alleged or adjudicated in which unscrupulous providers have persuaded Medicare recipients into accepting services or items in exchange for their Medicare identification numbers. These providers then used the beneficiaries' identification numbers to bill Medicare for other procedures or services not rendered. Beyond these limitations, HCFA data show that fraud units devoted 70 percent of their time responding to almost 100,000 beneficiary complaints during 1994, and over 5,000 complaints were referred to the HHS OIG for further investigation and possible prosecution. This workload may also increase as the volume of claims continues to rise, and thus, may necessitate a reevaluation on how these complaints are handled.

Sophisticated New Technology Available to Complement HCFA Initiatives

Commercial vendors have developed specialized antifraud systems that are much more sophisticated than the electronic controls used by Medicare carriers. Although it is too early to fully quantify the benefits of this new technology, one carrier's experience suggests that this technology has greater fraud-detection capabilities and can complement carriers' existing controls against fraud.

Antifraud System Offers Opportunities to Improve Detection and Prevention of Medicare Fraud

The antifraud systems recently developed and implemented by the private sector appear promising in identifying potentially fraudulent providers. We identified three vendors involved in developing such systems which incorporate a wide array of technologies to evaluate data and identify provider behavior patterns consistent with known attempts at fraud. Antifraud systems can formulate preliminary conclusions about both these patterns and their relative significance for further investigation. Although HCFA has recently acknowledged the importance of antifraud technology, it has not yet formally directed carriers to obtain it. Table 1 highlights some of the technical tools currently being used in antifraud systems.

Table 1: Technical Tools Used in Antifraud Systems

Technical tool	Description
Artificial intelligence	A form of computing used to develop programs that emulate the way humans solve problems, learn from experience, and make reasonable inferences from incomplete information.
Fuzzy logic	A form of logic used in some expert systems and other artificial-intelligence applications that processes data by monitoring very subtle degrees of abnormality for any given behavior. This technology weights factors and measures them collectively to reach certain conclusions and is suitable for detecting potential fraud and abuse because it takes into account many different factors at once. For example, the number or percentage of patient visits to a provider on Sundays and holidays can be combined and weighted with other data, such as the number of duplicate bills submitted. This information is then scored and measured against a peer group score.
Link analysis	A powerful visual tool that allows one to uncover, analyze, and display patterns of interaction among individuals and groups. These patterns are displayed by linking diagrams or two-dimensional shapes that represent an entity (e.g., patients, providers, etc.) with lines to display relationships. For example, one pattern may identify providers who over-refer patients to other providers because of possible kickbacks or collusion between providers.
Neural network (pattern recognition)	A type of artificial intelligence system intended to simulate the way in which a brain processes information, learns, and remembers. Neural networks learn by comparing new data to what has already been experienced, and can be used to detect hidden patterns in large volumes of data. They can learn characteristics of potentially fraudulent claims and quickly identify claims and providers suspected of fraud. Neural networks can identify, for instance, all providers who have a post office box mailing address, did not pass the usual certification boards, and for whom all patients seen have at least one lab test in common. Neural networks can also automatically learn new characteristics of potentially fraudulent claims, thereby updating their capabilities over time.

Sources: Computer Dictionary 2nd Edition, Microsoft Press, Redmond, Washington, 1994; and product descriptions from Booz-Allen & Hamilton, Inc.; Healthcare Information Services Team; and International Business Machines, Inc.

In many respects, antifraud technology can complement the current controls used by carriers. Antifraud technology allows looking at a number of variables concurrently to assess the validity of claims and whether the data display patterns of potential fraud. In addition, while medical review systems typically only look at a specific service, antifraud technology can look at entire episodes of care so that a service performed in the right context becomes apparent. For example, referrals for radiological services would typically originate with other providers, entail analysis of x-rays by other practitioners, and involve at least some follow-up treatment of some beneficiaries. If a provider continues to bill for radiological procedures without the full range of expected relationships and services for the beneficiaries, an antifraud system can monitor this activity or target the provider for further inquiry. Once a provider is suspected of potential fraud, future claims submitted by this provider may be suspended from claims processing to prevent additional losses.

Fraudulent providers must mirror many different behaviors to be consistent with legitimate providers—both in their prescribing habits and relationships with other providers—which makes it more difficult to avoid detection by this new technology. For example, to avoid detection by this technology, a fraudulent provider may have to ensure that (1) the bills submitted for a patient are for services consistent with other treatments received by the patient, (2) the sequence and timing of the patient's Medicare bills makes sense, and (3) referring providers listed on claims forms are also billing for that patient's care.

In addition to HCFA's existing controls, antifraud systems may also be a valuable component for its planned Medicare Transaction System (MTS), primarily a claims-processing system that is expected to be in use about 1999. According to HCFA's director of operations, MTS will increase Medicare's ability to detect potential fraud and abuse by providing a uniform claims format, integrated Medicare part A and B claims processing, and some standard statistical data analysis functions. Although HCFA is reviewing new emerging technologies, it has not yet determined whether antifraud technology will become part of MTS or how this technology would be acquired.

Private Health Insurers, One Medicare Carrier Using Latest Technology

Sophisticated, new antifraud technology is being used by several private health insurers, and early results have been positive. Several Medicare carriers—Aetna, CIGNA, and Travelers—have incorporated antifraud systems for their own private insurance business. According to a CIGNA official, its antifraud system has made fraud detection and investigation faster and easier. The assistant vice president of Aetna Health Plans stated that antifraud systems can yield a significant return on investment.

One carrier, Pennsylvania Blue Shield (PBS), has acquired an antifraud system for its Medicare operations.[6] Both identified potential fraud and actual savings from improper payments not made showed marked increases. PBS advised us that since the system's implementation in April 1994, it has identified over $6 million in overpayments due to potentially fraudulent claims. The carrier also reported that it more than doubled actual savings (from payments not made to suspicious providers), from over $2 million in 1993 to almost $5 million in 1994. This is a principal advantage because once a fraudulent pattern is identified, prepayment claims suspension for the suspect provider can be applied to the claims processing system. If the suspicion is confirmed, this claims suspension avoids additional losses to Medicare. Another benefit PBS associated with the system is a significant reduction in time needed to develop potential fraud cases.

The antifraud system used by PBS allows the carrier with the opportunity to identify fraudulent patterns of billing behavior. Since not all behaviors deserve equal weight in determining potential fraud, the carrier assigns each pattern a different weight, on the basis of its judgment and experience. The antifraud system identifies providers whose scores fall significantly above those of their peers in the same medical specialty.

One potentially fraudulent case identified by PBS' system concerned an ambulance service—an historically high-risk area for potential fraud. The ambulance company scored significantly high in 12 of 18 potentially fraudulent behavior patterns. PBS' antifraud system ranked the company particularly high in behavior patterns, such as percentage of trips out of the area in which the patient lives, average cost per patient, and other behavior patterns that could indicate nonhospital transports. Based on its investigation, PBS alleged that the company was inflating its Medicare reimbursements by using a different state identification number than the one for the state in which it was actually rendering services. This difference alone resulted in the company's charging about $70 more for each of about 23,000 trips, amounting to reimbursement of $1.6 million. PBS' fraud unit staff also suspected that almost half of the claims submitted by the company in a 6-month period were for transports not covered by Medicare.[7] While payment for many of these claims was initially denied by the carrier's claims processing system, to make the claims payable, the

[6] PBS, which is now referring to its Medicare operations as Xact Medicare Services, is the largest Medicare part B carrier, having processed over 74 million claims in 1994.

[7] Medicare covers ambulance transports to or from a hospital or skilled nursing facility only.

provider allegedly modified the patient's destination to reflect a hospital transport.

The data generated by the antifraud system allowed the carrier to immediately refer the case to the HHS OIG for further investigation. This case has been accepted by one of the U.S. attorneys for Pennsylvania, who is pursuing a criminal investigation. These suspicions materialized quickly with this new complex technology, which combines an analytical tool—fuzzy logic (see table 1)—with high-performance computing[8] and statistics to identify high-risk providers within peer groups. According to the vendor, the cost to purchase a system similar to the one used by PBS would range from $315,000 to $400,000, depending on current hardware configuration, level of customization needed, installation, training, and support.

Rising Medicare Fraud in Florida Offers Opportunity for Operational Test of Antifraud Technology

Despite efforts to halt rising fraud, information from HCFA, law enforcement agencies, carriers, and health insurance organizations, indicates that Medicare fraud in Florida has mushroomed out of control over the past few years and may be costing taxpayers hundreds of millions of dollars every year. The South Florida area has been a particular target of fraud against Medicare. In response, HCFA formed the interagency South Florida Workgroup to coordinate the efforts to stop this fraud. Antifraud technology, too, might help considering the complex nature of health care fraud and the many types of schemes perpetrated against Medicare.

Florida's Medicare Fraud Schemes

Florida has been reported to have the highest rate of Medicare fraud in the nation. According to its U.S. attorney, the state has been particularly victimized by Medicare fraud due to the large percentage of poor and elderly people in the area. With only 7 percent of the Medicare beneficiary population, Florida accounted over 20 percent (about $12 billion) of total fiscal year 1993 Medicare part B spending (about $54 billion). Further, Florida's Medicare carrier identified about $21 million in overpayments for potential fraudulent claims during 1994—about half the total $46 million identified by carrier fraud units nationwide.

During a hearing on health care fraud in March 1995, Florida's U.S. attorney described Medicare fraud in South Florida as rampant. Particular schemes have included (1) offering beneficiaries free groceries, medical

[8] High-performance computing refers to the use of advanced computing technologies, including hardware and software that solve highly complex, numerically intensive problems quickly.

services, or cash in exchange for Medicare identification numbers that can be used to fraudulently bill the program, (2) using physicians' names and identification numbers to submit fraudulent claims, and (3) applying for and obtaining Medicare physician/supplier identification numbers though not authorized or licensed as a health care provider.

One Florida company that allegedly existed just to bill Medicare without rendering medical services was paid about $2 million during a 5-month period. By the time this scheme was detected and a court order obtained to freeze the company's bank account, most of the $2 million had disappeared—as had the company's owner. Table 2 provides examples of other recent Medicare fraud cases in Florida, as reported by the Department of Justice in 1994.

Table 2: Examples of Medicare Fraud Cases Recently Adjudicated in Florida

Provider type	Description
Home health	In October 1994, an owner and operator of a home health agency was sentenced to 37 months in prison, fined $100,000, and ordered to forfeit real and personal property valued at approximately $750,000. Through his home health agency, the defendant submitted thousands of Medicare claims that falsely stated that licensed, medical doctors ordered health services for Medicare patients. The indictment alleged that the defendant received $1.4 million in Medicare reimbursements from 1990 through 1993.
Lab services	In September 1994, five defendants were sentenced after pleading guilty to scheming to defraud the Medicare and Medicaid programs out of approximately $4 million. The lead defendant admitted that she routinely purchased Medicare and Medicaid information and often paid people to undergo various tests. She used this information to submit fraudulent claims. Two other defendants admitted that, as diagnostic technicians working for the lead defendant, they performed 98 diagnostic tests on each other to generate additional test results, which were used as a basis for false claims submissions.
Home infusion therapy	Twelve defendants were convicted and sentenced for defrauding Medicare of over $14 million from 1989 through 1991. The principal defendants owned and operated eight companies in Miami, which distributed (usually to the home) nutritional supplements to Medicare beneficiaries. However, these supplements are only covered by Medicare if a beneficiary is unable to eat solid foods. Doctors who signed blank prescriptions and door-to-door recruiters who fraudulently obtained Medicare beneficiary numbers in exchange for free liquid nutrients described as "milk" were also convicted.

Source: Department of Justice Health Care Fraud Report, Fiscal Year 1994.

HCFA's South Florida Initiative

To coordinate the South Florida antifraud effort, in September 1994, HCFA formed the South Florida Workgroup. The workgroup has undertaken the "South Florida Project" to identify specific problems and recommend corrections. Participants include Medicare contractors in Florida, the HHS OIG, the Federal Bureau of Investigation, Justice, Miami's United States attorney, and the Florida Attorney General's Medicaid fraud control unit. The workgroup made recommendations to the HCFA Administrator this spring.

One issue addressed by the workgroup concerns a problem identified in July 1994, in which 335 potentially fraudulent applications for provider numbers were discovered by chance during a manual review of pending applications. If these suspicious applications had been approved, each provider number would have created additional opportunities for perpetrators to fraudulently bill Medicare. Weaknesses in the provider enrollment process[9] have also contributed to Medicare's vulnerability to fraud, particularly in Florida. HCFA's controls for monitoring the process had been weak; it was, therefore, easy for fraudulent providers to obtain and retain credentials that allowed them to be paid by Medicare. The HCFA task force has already taken several actions to strengthen the conditions of enrollment, such as verifying addresses, telephone numbers, and other information submitted by the applicant.

Antifraud Technology May Benefit Florida's Carrier

The following example illustrates how losses to Medicare fraud can occur, and how antifraud technology can prevent such losses. In one recent and highly publicized case in South Florida, an unemployed tow-truck driver was charged with using a nonexistent medical laboratory to cheat Medicare out of more than $300,000 by allegedly filing 717 false electronic claims in just 2 weeks. According to investigators, the suspect was arrested as he tried to withdraw $200,000 in cash from his "company's" bank account. If not for the actions of a suspicious bank teller, investigators say, the suspect would have disappeared. An additional $300,000 in electronic claims from this same individual were in process, but had not yet been paid at the time of his arrest.

We discussed this case with several antifraud system vendors, who confirmed that their technology could have detected this type of fraud. According to one company representative, antifraud systems can identify individuals in this type of scheme if a combination of behavior patterns is established in the system to evaluate all new Medicare billers. For instance, if the patterns included all new providers having a post office box (in lieu of a street address) combined with a high number of first-time claims and a large number of beneficiaries located very long distances from the place of service, the provider in this example would have matched known behavior patterns consistent with attempted fraud.

In its current efforts to combat Medicare fraud in Florida, HCFA acquired an advanced data query system. Although the capabilities of this system are

[9] Medicare and Medicaid: Opportunities to Save Program Dollars by Reducing Fraud and Abuse (GAO/T-HEHS-95-110, March 22, 1995).

substantial for medical review and reporting functions, it does not include the capabilities available through antifraud technology to draw inferences regarding potential fraud. The substantial losses attributable to the Florida fraud problem provide HCFA with an opportunity to test the effectiveness of this latest antifraud technology in reducing Medicare fraud.

Conclusions

Medicare continues to experience large losses each year due to fraud. Existing risks are sharply increased by the continual growth in Medicare claims—both in number and percentage processed electronically. Existing Medicare payment safeguard controls can be bypassed and apparently do not deter fraudulent activities. HCFA should be able to benefit by taking full advantage of the emerging antifraud technology to better identify and prevent Medicare fraud. The number and types of Medicare fraud schemes perpetrated in South Florida may make that area the best place to test antifraud systems before nationwide use.

Recommendation

To assist the Health Care Financing Administration in identifying more potential fraud in the Medicare program, we recommend that the Secretary of Health and Human Services direct the Administrator of HCFA to develop a plan for implementing antifraud technology. One approach would be to monitor the carrier currently using antifraud technology and immediately begin a pilot or demonstration program that would enable the agency to quickly see through valuable, first-hand experience how it can best deploy antifraud technology. Such a test could be conducted where the need to reduce fraud is great, such as in South Florida. If the results of this test show that antifraud technology is cost effective and useful in identifying potential fraud, HCFA should expeditiously expand the use of this technology nationwide.

Agency Comments and Our Evaluation

In commenting on a draft of this report, HHS agreed that Medicare payment safeguards could benefit from new technology to identify fraudulent patterns of behavior. However, it expressed concerns about implementing such technology in the Medicare program because it questions the (1) general applicability of this technology in a health insurance setting, (2) utility of the technology to Medicare without substantial modification, and (3) degree to which this technology has been tested. HHS did not respond to our recommendation to develop a plan to implement such technology. It stated that it would continue to review antifraud technology for possible inclusion in its Medicare Transaction System (MTS), now scheduled for implementation in 1999.

As noted in our report, these new antifraud technologies are gradually being adopted by private health insurers. On several occasions during our fieldwork, and at our final conference with HCFA officials, we discussed the use of this technology by Pennsylvania Blue Shield—the largest Medicare carrier. In addition, HCFA officials attended a number of demonstrations of this technology sponsored by the carrier. Since we completed our audit work, several additional private health insurers have contracted for this type of technology, and we have given HCFA a list of these companies.

We believe that, as would be the case with almost any system, customization—along with its costs—may be needed to satisfy specific program requirements. If Medicare is to be proactive in detecting and preventing fraud, it must continually modify its systems' capabilities to keep pace with new fraud schemes and the changing health care environment. While Pennsylvania Blue Shield noted that certain modifications were necessary to tailor the system's behavior patterns to fit Medicare's needs, the acquisition price included the costs for this customization. According to the vendor, the cost for a similar system would range from $315,000 to $400,000, depending on factors such as the numbers and types of potential fraud scenarios that need to be incorporated into the software, and a client's particular hardware configuration. HCFA has invested in developing fraud behavior profiles for one carrier and, according to the vendor, this information is available to other Medicare carriers at no additional cost.

HHS noted that HCFA is actively reviewing antifraud technology but stated that the results of its review indicate that more testing is needed before any judgment on the usefulness of this technology in detecting Medicare fraud can be made. Pennsylvania Blue Shield has reported considerable success with this technology, returning funds to the Medicare Trust Fund. The carrier advised HCFA that it collected over $94,000 in overpayments, and informed us that it identified over $6 million in potential fraud as a result of cases identified by its antifraud system since the system's implementation in April 1994. Thus, the application of antifraud technology to the Medicare program appears to be cost-effective. A strong indication of its value is that other insurance companies are moving to acquire similar technology.

Given the potential for substantial savings of program funds and commonly accepted best practices in the field of information resources management that encourage the use of available off-the-shelf software, we continue to believe that HCFA should expeditiously expand acquisition and testing of this technology in the Medicare program. In an era of escalating health care costs, rising indicators of fraud, and a new market with several competing vendors, it appears prudent and practical to acquire such technology, starting in the higher risk environments, such as Florida.

As agreed with your office, unless you publicly announce the contents of this report earlier, we will not distribute it until 30 days from the date of this letter. We will then send copies of this report to other interested congressional committees; the Secretary of Health and Human Services; the Administrator of the Health Care Financing Administration; the Director of the Office of Management and Budget; and the 32 Medicare carriers. Copies will also be made available to others upon request. Should you have any questions concerning this report, please contact me at (202) 512-6408. Other major contributors to the report are listed in appendix III.

Sincerely yours,

Frank Reilly

Frank W. Reilly
Director, Information Resources Management/
Health, Education, and Human Services

Contents

Tables

Figures

Abbreviations

GAO	General Accounting Office
HCFA	Health Care Financing Administration
HHS	Department of Health and Human Services
MTS	Medicare Transaction System
OIG	Office of Inspector General
PBS	Pennsylvania Blue Shield

Appendix I

Scope and Methodology

To accomplish our objectives, we obtained information on the antifraud activities of all 32 Medicare part B carrier fraud units. We visited the following 10 fraud units and interviewed unit managers and staff to determine how information technology is being used to detect and prevent potential Medicare fraud: Blue Shield (Alabama); Travelers (Connecticut); Blue Shield (Florida); Aetna (Georgia); Health Care Service Corporation (Illinois); AdminaStar (Kentucky); Blue Shield (Maryland); General American Life (Missouri); Blue Shield (New York); and Blue Shield (Pennsylvania). In some cases, we also met with representatives from carriers' claims processing and medical review units to obtain information on the process for referring suspected fraud cases to the fraud units. We also surveyed the remaining 22 carriers by telephone to determine the types of technology they use.

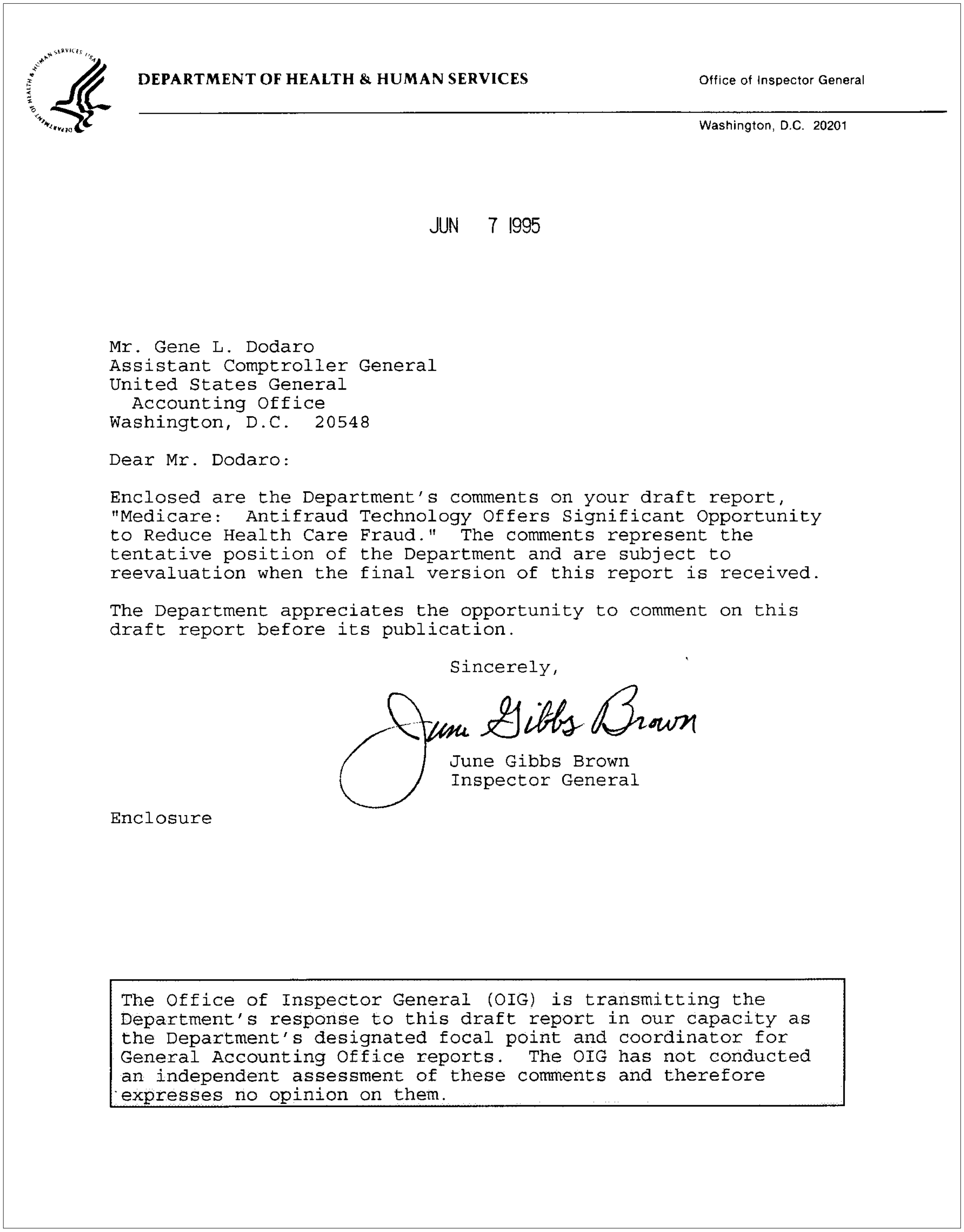
We interviewed HCFA officials from the Bureau of Program Operations to identify fraud-unit requirements, guidance, and funding, and how units are evaluated under HCFA's Contractor Performance Evaluation Program. We also met with the project manager for the planned Medicare Transaction System (MTS) to determine whether this system will include antifraud technology. To obtain additional information on health care antifraud activities throughout the government, we met with officials from the HHS OIG and the Department of Justice, in Washington, D.C.

To obtain data on private industry antifraud capabilities, we met with representatives of Medicare carriers' private insurance business units in Middletown and East Hartford, Connecticut. In addition, we interviewed representatives of the Health Care Insurance Association of America and the National Health Care Anti-Fraud Association, in Washington, D.C., to obtain background information on health care fraud and the programs private insurers use to combat fraud. We also met with companies developing specific technology to detect health care fraud.

Appendix II

Comments From the Department of Health and Human Services

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of Inspector General

Washington, D.C. 20201

JUN 7 1995

Mr. Gene L. Dodaro
Assistant Comptroller General
United States General
  Accounting Office
Washington, D.C. 20548

Dear Mr. Dodaro:

Enclosed are the Department's comments on your draft report, "Medicare: Antifraud Technology Offers Significant Opportunity to Reduce Health Care Fraud." The comments represent the tentative position of the Department and are subject to reevaluation when the final version of this report is received.

The Department appreciates the opportunity to comment on this draft report before its publication.

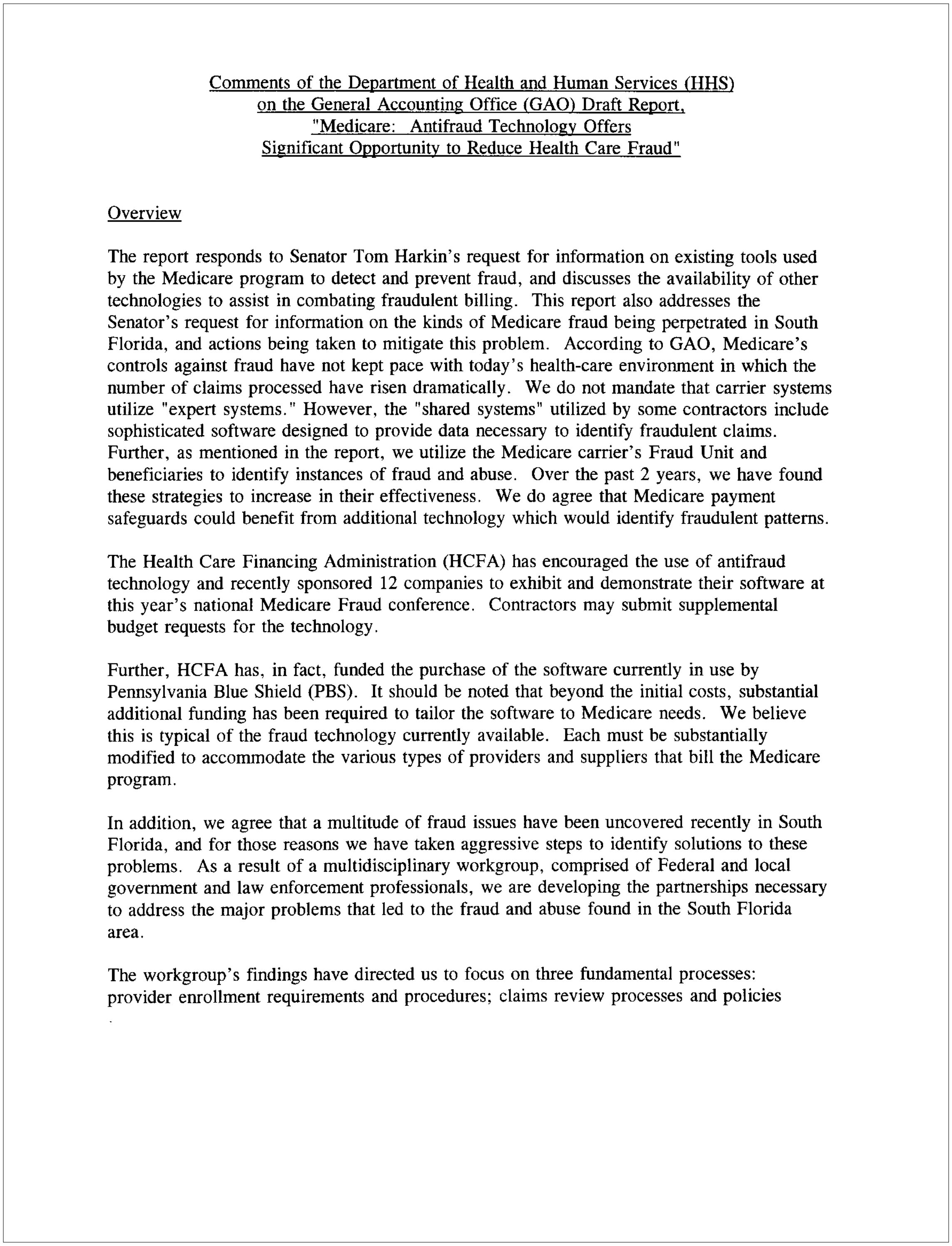
Sincerely,

June Gibbs Brown

June Gibbs Brown
Inspector General

Enclosure

The Office of Inspector General (OIG) is transmitting the Department's response to this draft report in our capacity as the Department's designated focal point and coordinator for General Accounting Office reports. The OIG has not conducted an independent assessment of these comments and therefore expresses no opinion on them.



Comments of the Department of Health and Human Services (HHS)
on the General Accounting Office (GAO) Draft Report,
"Medicare: Antifraud Technology Offers
Significant Opportunity to Reduce Health Care Fraud"

Overview

The report responds to Senator Tom Harkin's request for information on existing tools used by the Medicare program to detect and prevent fraud, and discusses the availability of other technologies to assist in combating fraudulent billing. This report also addresses the Senator's request for information on the kinds of Medicare fraud being perpetrated in South Florida, and actions being taken to mitigate this problem. According to GAO, Medicare's controls against fraud have not kept pace with today's health-care environment in which the number of claims processed have risen dramatically. We do not mandate that carrier systems utilize "expert systems." However, the "shared systems" utilized by some contractors include sophisticated software designed to provide data necessary to identify fraudulent claims. Further, as mentioned in the report, we utilize the Medicare carrier's Fraud Unit and beneficiaries to identify instances of fraud and abuse. Over the past 2 years, we have found these strategies to increase in their effectiveness. We do agree that Medicare payment safeguards could benefit from additional technology which would identify fraudulent patterns.

See comment 1.

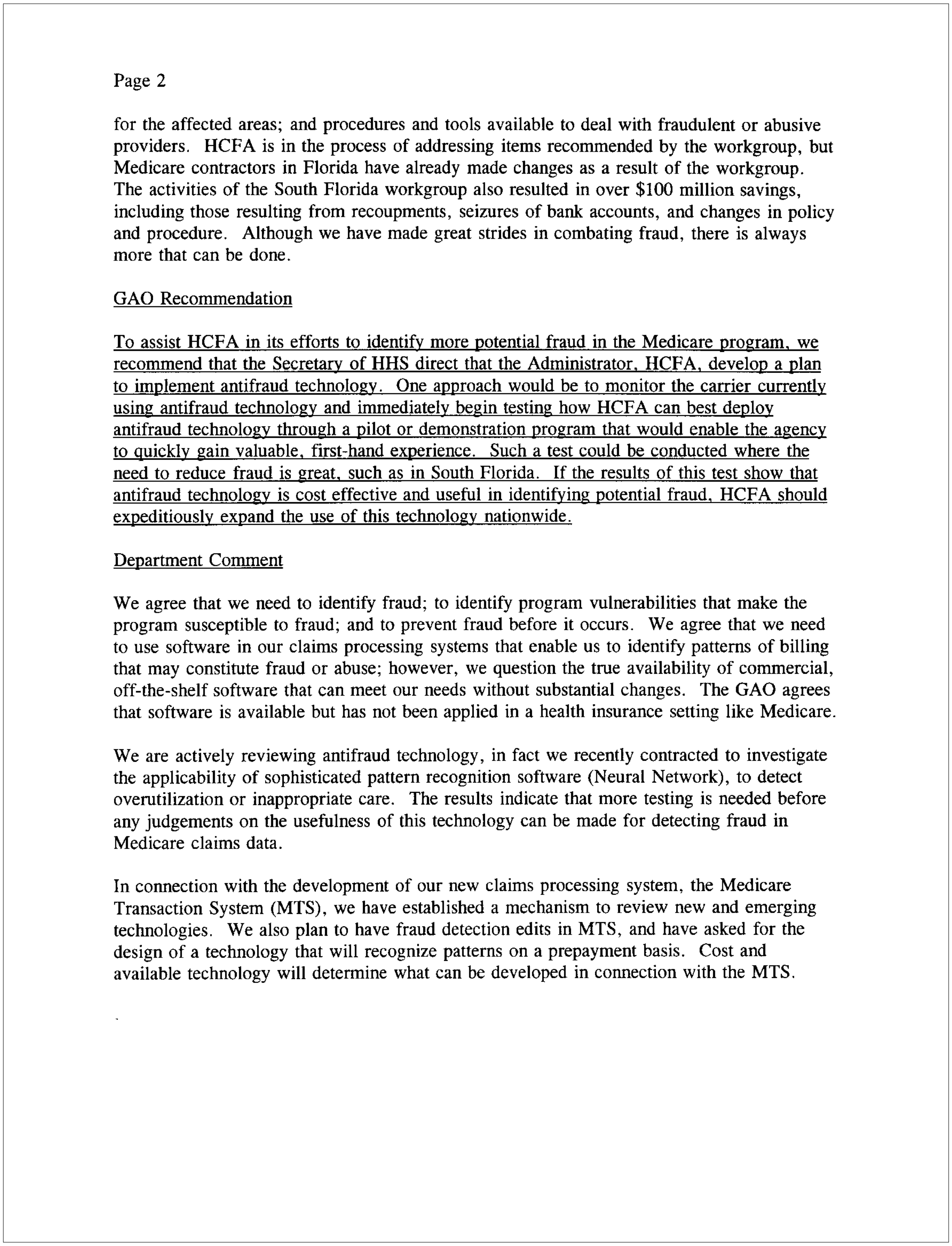
The Health Care Financing Administration (HCFA) has encouraged the use of antifraud technology and recently sponsored 12 companies to exhibit and demonstrate their software at this year's national Medicare Fraud conference. Contractors may submit supplemental budget requests for the technology.

Further, HCFA has, in fact, funded the purchase of the software currently in use by Pennsylvania Blue Shield (PBS). It should be noted that beyond the initial costs, substantial additional funding has been required to tailor the software to Medicare needs. We believe this is typical of the fraud technology currently available. Each must be substantially modified to accommodate the various types of providers and suppliers that bill the Medicare program.

In addition, we agree that a multitude of fraud issues have been uncovered recently in South Florida, and for those reasons we have taken aggressive steps to identify solutions to these problems. As a result of a multidisciplinary workgroup, comprised of Federal and local government and law enforcement professionals, we are developing the partnerships necessary to address the major problems that led to the fraud and abuse found in the South Florida area.

See comment 2.

The workgroup's findings have directed us to focus on three fundamental processes: provider enrollment requirements and procedures; claims review processes and policies



for the affected areas; and procedures and tools available to deal with fraudulent or abusive providers. HCFA is in the process of addressing items recommended by the workgroup, but Medicare contractors in Florida have already made changes as a result of the workgroup. The activities of the South Florida workgroup also resulted in over $100 million savings, including those resulting from recoupments, seizures of bank accounts, and changes in policy and procedure. Although we have made great strides in combating fraud, there is always more that can be done.

GAO Recommendation

To assist HCFA in its efforts to identify more potential fraud in the Medicare program, we recommend that the Secretary of HHS direct that the Administrator, HCFA, develop a plan to implement antifraud technology. One approach would be to monitor the carrier currently using antifraud technology and immediately begin testing how HCFA can best deploy antifraud technology through a pilot or demonstration program that would enable the agency to quickly gain valuable, first-hand experience. Such a test could be conducted where the need to reduce fraud is great, such as in South Florida. If the results of this test show that antifraud technology is cost effective and useful in identifying potential fraud, HCFA should expeditiously expand the use of this technology nationwide.

Department Comment

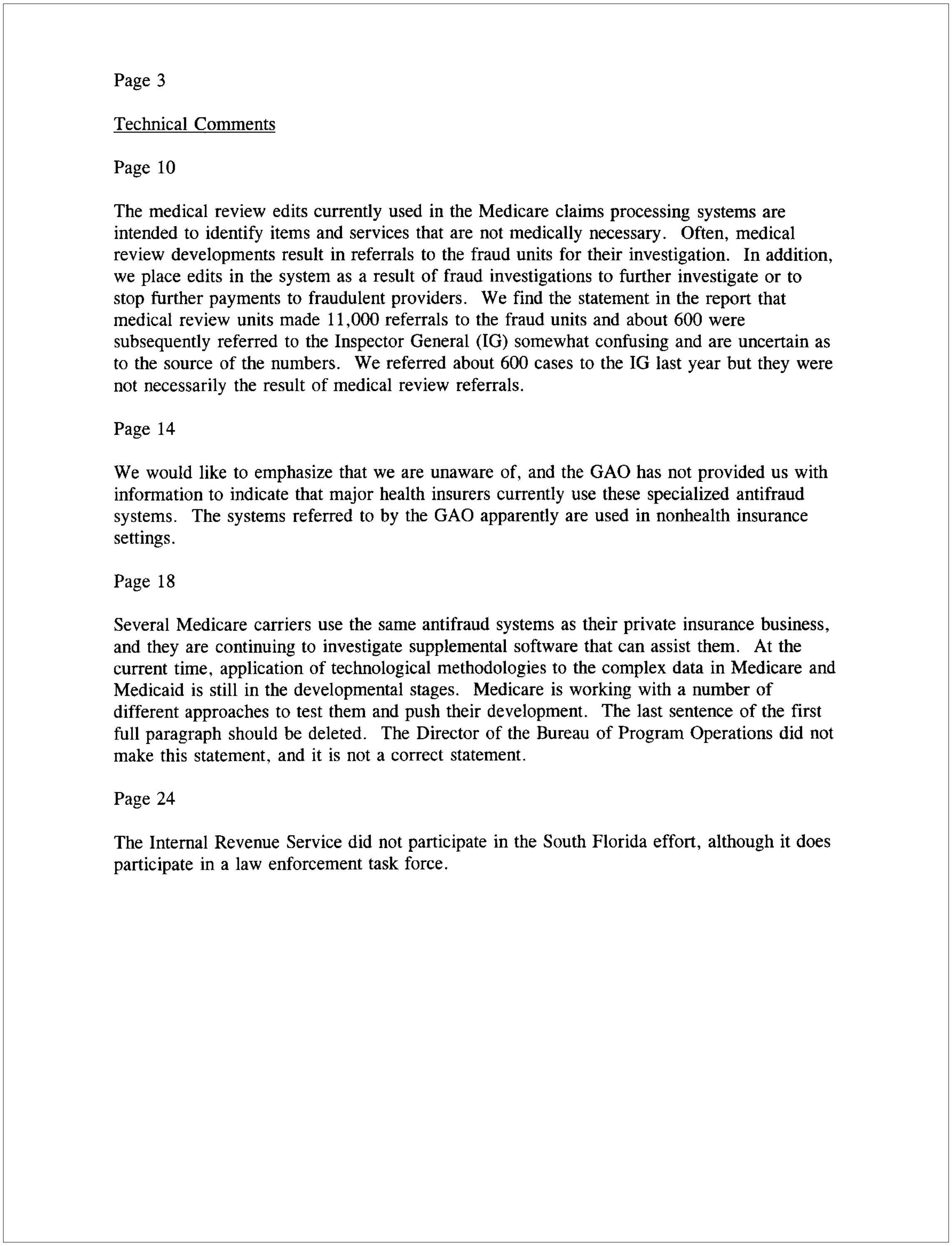
See comment 3.

We agree that we need to identify fraud; to identify program vulnerabilities that make the program susceptible to fraud; and to prevent fraud before it occurs. We agree that we need to use software in our claims processing systems that enable us to identify patterns of billing that may constitute fraud or abuse; however, we question the true availability of commercial, off-the-shelf software that can meet our needs without substantial changes. The GAO agrees that software is available but has not been applied in a health insurance setting like Medicare.

We are actively reviewing antifraud technology, in fact we recently contracted to investigate the applicability of sophisticated pattern recognition software (Neural Network), to detect overutilization or inappropriate care. The results indicate that more testing is needed before any judgements on the usefulness of this technology can be made for detecting fraud in Medicare claims data.

See comment 4.

In connection with the development of our new claims processing system, the Medicare Transaction System (MTS), we have established a mechanism to review new and emerging technologies. We also plan to have fraud detection edits in MTS, and have asked for the design of a technology that will recognize patterns on a prepayment basis. Cost and available technology will determine what can be developed in connection with the MTS.



Page 3

Technical Comments

Page 10

See comment 5.

The medical review edits currently used in the Medicare claims processing systems are intended to identify items and services that are not medically necessary. Often, medical review developments result in referrals to the fraud units for their investigation. In addition, we place edits in the system as a result of fraud investigations to further investigate or to stop further payments to fraudulent providers. We find the statement in the report that medical review units made 11,000 referrals to the fraud units and about 600 were subsequently referred to the Inspector General (IG) somewhat confusing and are uncertain as to the source of the numbers. We referred about 600 cases to the IG last year but they were not necessarily the result of medical review referrals.

Page 14

See comment 6.

We would like to emphasize that we are unaware of, and the GAO has not provided us with information to indicate that major health insurers currently use these specialized antifraud systems. The systems referred to by the GAO apparently are used in nonhealth insurance settings.

Page 18

See comment 7.

Several Medicare carriers use the same antifraud systems as their private insurance business, and they are continuing to investigate supplemental software that can assist them. At the current time, application of technological methodologies to the complex data in Medicare and Medicaid is still in the developmental stages. Medicare is working with a number of different approaches to test them and push their development. The last sentence of the first full paragraph should be deleted. The Director of the Bureau of Program Operations did not make this statement, and it is not a correct statement.

Page 24

See comment 8.

The Internal Revenue Service did not participate in the South Florida effort, although it does participate in a law enforcement task force.

GAO Comments

1. We disagree with HHS' statement that shared systems or claims processing systems used by some contractors include sophisticated software designed to provide data necessary to identify fraudulent claims. As our report discusses, while these systems have some capabilities that may identify potential fraud, including suspending duplicate claims, these systems were primarily designed to process and pay Medicare claims. We have also testified and reported on limitations of these systems compared with private-sector capabilities.[1]

2. We commend HCFA for coordinating its antifraud efforts in South Florida. The amounts recovered and the examples cited in our report confirm the serious nature of the fraud plaguing the Medicare program in South Florida. We believe that the types of fraud schemes identified lend themselves to the antifraud technology we recommended be extended to South Florida.

3. As discussed in the Agency Comments and Our Evaluation section of this report, HHS officials were aware of the existence and application of this type of technology in the health insurance setting.

4. HHS indicates that HCFA is planning to incorporate fraud detection edits in MTS and has asked for the design of a technology that will recognize patterns on a prepayment basis. However, MTS is not scheduled to be implemented until 1999. Also, as our report points out, antifraud technology is available, and current best practices in information systems development recommend taking a hard look at commercially available technology, and in fact favor its acquisition over specific in-house development efforts.

5. We have updated our report to reflect current fiscal year 1994 data. Also, because HCFA combines referrals from providers, medical review, and special requests from the OIG and HCFA into one category, HCFA could not provide us with the number of potential fraud referrals made specifically by medical review or those referrals subsequently referred to the OIG.

6. Discussed in the Agency Comments and Our Evaluation section of this report.

7. We have deleted the statement we attributed to the Director of the Bureau of Program Operations and clarified that although HCFA is

[1] Medicare Claims Billing Abuse: Commercial Software Could Save Hundreds of Millions Annually (GAO/T-AIMD-95-133, May 5, 1995); Medicare Claims (GAO/AIMD-95-135).

reviewing emerging technologies, it has not yet determined whether antifraud technology will be applied to MTS or whether this technology would be developed in-house or acquired via a commercial system.

8. We have revised the report by deleting the Internal Revenue Service from the list of participants involved in the South Florida Workgroup.

Appendix III

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

Patricia T. Taylor, Associate Director
David B. Alston, Assistant Director
Yvette R. Banks, Evaluator-in-Charge
Theodore P. Alves, Technical Adviser
Michael P. Fruitman, Communications Analyst
Teresa L. Jones, Information Processing Specialist

Atlanta Regional Office

Carl L. Higginbotham, Senior Evaluator
Amanda S. Cooksey, Staff Evaluator
Maria B. Warkentine, Staff Evaluator

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 6015
Gaithersburg, MD 20884-6015

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000
or by using fax number (301) 258-4066, or TDD (301) 413-0006.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (301) 258-4097 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

PRINTED ON RECYCLED PAPER