United States General Accounting Office

GAO

Report to the Ranking Minority Member, Subcommittee on National Security, International Affairs and Criminal Justice, House Committee on Government Reform and Oversight

May 1996

HEALTH CARE FRAUD

Information-Sharing Proposals to Improve Enforcement Efforts

GAO/GGD-96-101

GAO

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

General Government Division

B-259795

May 1, 1996

The Honorable Karen L. Thurman
Ranking Minority Member
Subcommittee on National Security,
International Affairs and Criminal Justice
Committee on Government Reform and Oversight
House of Representatives

Dear Ms. Thurman:

In response to the former Chairman's request and subsequent agreements with you, this report focuses on information-sharing issues that may affect health care anti-fraud enforcement efforts. Specifically, the report discusses (1) the extent of federal and state immunity laws protecting persons who report health care fraud-related information and (2) the evidence that exists for and against establishing a centralized health care fraud database to enhance information sharing and support enforcement efforts.

We are sending copies of this report to the Attorney General, appropriate congressional committees, and other interested parties. Copies will also be made available to others upon request.

The major contributors to this report are listed in appendix VII. If you or your staff have any questions about this report, please contact me on (202) 512-8777.

Sincerely yours,

Norman Rabkin

Norman J. Rabkin
Director, Administration
of Justice Issues

Executive Summary

Purpose

Health care fraud burdens the nation with enormous financial costs, while threatening the quality of health care. Estimates of annual losses due to health care fraud range from 3 to 10 percent of all health care expenditures—between $30 billion and $100 billion based on estimated 1995 expenditures of over $1 trillion. In late 1993, the Attorney General designated health care fraud as the Department of Justice's number two enforcement priority, second only to violent crime initiatives.

In response to a request from the former Chairman and subsequent agreements with the current Ranking Minority Member, House Subcommittee on National Security, International Affairs and Criminal Justice, Committee on Government Reform and Oversight, GAO's report focuses on information-sharing issues that may affect health care anti-fraud enforcement efforts. Specifically, this report discusses (1) the extent of federal and state immunity laws protecting persons who report health care fraud-related information and (2) the advantages and disadvantages of establishing a centralized health care fraud database to enhance information sharing and support enforcement efforts.

Background

The size and complexity of the health care industry present considerable challenges for government and industry fraud investigators. Federal enforcement agencies responsible for investigating health care fraud include the Federal Bureau of Investigation (FBI); the U.S. Postal Inspection Service; and various Offices of Inspector General, such as that within the Department of Health and Human Services (HHS). Moreover, most states have established insurance fraud bureaus or units that investigate health care fraud. Also, many private insurance carriers have established special units to investigate fraud within their health plans. In addition, a group of private sector health insurers and public sector enforcement agencies has established the National Health Care Anti-Fraud Association (NHCAA), which represents a cooperative effort to address health care fraud.

Over the years, the administration and Congress have considered proposals to enhance information sharing among the federal, state, and private entities involved in health care anti-fraud enforcement. In considering such proposals, decisionmakers have been confronted with the inherent conflicts between the dual public policy goals of (1) supporting the role of private entities in the investigation and prosecution of fraud and (2) protecting innocent people and organizations against unsubstantiated allegations made in bad faith or with malice. On

the one hand, some proposals have called for federal immunity legislation to provide protection—from defamation of character and other civil lawsuits—for persons (including private insurance company employees) who report suspected fraud. The purpose of such immunity law would be to encourage the reporting of suspected fraud to law enforcement agencies.

On the other hand, concerns have been raised about the need to incorporate safeguards to provide individuals with protection against bad faith allegations. Safeguards that have been considered include requirements governing the specificity and credibility of reported information and provisions giving individuals legal recourse against bad faith allegations that could seriously damage an individual's life and livelihood if publicly disclosed.

Other proposals have called for establishment of a national, centralized database of health care fraud-related information. The purpose of such a database would be to coordinate federal, state, and local anti-fraud enforcement efforts by providing a national data collection program for information about persons or entities involved in health care fraud.

To obtain perspectives on these issues, GAO contacted key government and private organizations.[1] GAO also surveyed all 50 state insurance commissioners.

Results in Brief

GAO identified no immunity provision on the federal level designed to protect persons who report suspected health care fraud to law enforcement agencies. One existing federal immunity provision would protect persons reporting health care fraud-related information, but it applies only to persons who report information about the Medicare and Medicaid programs to peer review contractors operating under those programs. Private insurers and other health care claims processors are provided no federal immunity protection for reporting health care fraud-related information concerning other public or private health plans. While most states have enacted immunity laws protecting insurers, these laws vary in terms of the protection provided. Legislation (S. 1088, 104th

[1]GAO visited 12 offices of federal agencies (U.S. Attorney, FBI, and Postal Inspection Service offices); 6 offices of state agencies (insurance departments, fraud bureaus, and attorney general offices); and 13 private insurance companies. Except for 2 insurers located in Connecticut and 3 in Illinois, all of the 31 offices visited were located in 4 judgmentally selected states—Florida, Maryland, Massachusetts, and Texas. GAO also contacted the American Medical Association, the Health Insurance Association of America, the National Insurance Crime Bureau, and the National Health Care Anti-Fraud Association.

Cong.) awaiting congressional consideration at the time of GAO's review would expand existing federal immunity law to protect persons providing information about fraud in any health plan (public or private) to either HHS or Justice.

Almost all of the federal and state officials—as well as representatives of insurance companies and health care providers—interviewed by GAO supported the concept of an expanded federal immunity law, including appropriate safeguards to protect against unsubstantiated allegations made in bad faith. The responses to GAO's survey of state insurance commissioners indicated broad support for both state and federal immunity laws. Many of the field officials GAO interviewed said that a federal immunity law, to be most useful, should be broader than the provisions included in S. 1088 by providing immunity protection to (1) persons sharing fraud-related information with any applicable federal or state enforcement entity and (2) insurers sharing such information with other insurers. Some of these officials noted that the latter approach involves greater risks because of the possibility that insurers could use the information inappropriately to discriminate against health care providers.

There is no centralized national database to track criminal activity in the health care system that would assist federal, state, and industry anti-fraud enforcement efforts. Recent congressional and administration proposals would have established health care fraud databases containing information about health care system participants (such as license revocations and criminal convictions) and ongoing health care fraud investigations, but none of these were implemented. S. 1088 proposes to establish a centralized health care fraud database of final adverse actions—including criminal convictions, civil judgments, and negative licensing or certification actions—accessible by federal and state government agencies and health insurers.

Most of the law enforcement and industry officials GAO interviewed saw benefits in and supported the establishment of a database of final adverse actions; however, many of the others did not consider the potential benefits essential to enforcement efforts. Many of the officials also suggested that enforcement benefits probably would accrue from centralized databases that contain information about (1) ongoing health care fraud investigations and/or (2) suspected fraud reported by persons to enforcement or regulatory agencies. However, officials were concerned that such databases pose risks in terms of unauthorized disclosure and use

of the information. In addition to these issues, there are also uncertainties about the costs of developing and operating a centralized database.

Principal Findings

Existing Federal and State Immunity Laws Are Limited

GAO identified no immunity provision on the federal level designed to protect persons who report health care fraud-related information to law enforcement agencies. One provision of the Social Security Act (codified at 42 U.S.C. 1320c-6(a)) would protect persons reporting fraud-related information about Medicare and Medicaid to HHS peer review contractors. However, this immunity provision is limited in terms of the protection it provides. For instance, the immunity law does not protect persons who report Medicare and Medicaid fraud directly to federal law enforcement authorities, such as the FBI or Postal Inspection Service. Further, it does not protect persons who report suspected fraud involving other public or private sector health plans.

State immunity laws also provide protection to persons reporting suspected health care fraud, but not all states have enacted such laws and the protection provided varies. Responses to GAO's July 1995 survey of state insurance commissioners revealed that 38 of the 50 states had enacted immunity laws protecting the sharing of health care fraud-related information. Twenty-four of the states specifically protect persons reporting fraud to state and federal agencies, but 10 states protect only persons reporting to state agencies. Eight states indicated that they provide immunity protection for insurers sharing information with other insurers. In each of the 38 states, the immunity provision is contingent on the absence of malice or bad faith on the part of the person reporting fraud.

Expanded Federal Immunity Law With Proper Safeguards Is Broadly Supported

A recent congressional immunity proposal, included in S. 1088, would expand existing federal immunity protection by protecting persons who report any public or private health care fraud-related information to either HHS or Justice. However, this proposed immunity does not address the reporting of fraud-related information to other government investigative and prosecutive entities involved in anti-fraud enforcement—including federal agencies such as the Postal Inspection Service and state agencies such as the offices of attorneys general. It also does not address

information sharing between insurance company investigative units, a protection that has been adopted in eight states.

Almost all of the officials GAO interviewed at 31 field locations in 6 states supported the concept of a broad federal immunity law with proper safeguards to protect against inappropriate use. These officials generally stated that such an immunity law would provide a consistent level of protection in all the states and might encourage more insurers to report suspected fraud to enforcement agencies. GAO's survey of state insurance commissioners also indicated broad support for an expanded federal immunity law, with the expectation that such a law would be effective in facilitating information sharing between insurers and enforcement/regulatory authorities. About half of the officials GAO interviewed favored expanding the current legislative proposal to protect (1) persons reporting fraud-related information to enforcement entities other than HHS and Justice and (2) insurers sharing fraud-related information with other insurers.

There was some negative reaction to the concept of an expanded federal immunity law. For example, one official believed state legislatures were adequately addressing this issue while another believed some insurers would, as a business decision, still avoid reporting suspected fraud. Cited as a potential drawback to providing immunity to insurers that share information with other insurers was the possibility that they could use the information inappropriately, such as to deny claims or disallow employment opportunities for physicians or other health care providers.

Centralized Database May Be Beneficial but Not Without Risk

There is no comprehensive source of health care fraud information that investigators can access to assist in their anti-fraud enforcement efforts. For example, the FBI's National Crime Information Center contains useful information about criminal histories, but it is accessible only by authorized enforcement agencies. Information maintained by the National Association of Insurance Commissioners is publicly available but deals only with insurance companies and agents, not health practitioners. NHCAA's Provider Indexing Network System contains information about enforcement actions taken against health providers, as well as ongoing health care fraud investigations. However, it is directly accessible only by NHCAA members and does not contain comprehensive nationwide information. To improve access to information about health care fraud, S. 1088 proposes to establish a national database of final adverse actions—i.e., criminal convictions, civil judgments, and negative licensing

or certification actions—taken against health care providers, suppliers, and practitioners. The database would be accessible by law enforcement and regulatory agencies and insurers.

Officials at 17 of the 31 field offices GAO visited indicated that they favored the establishment of a centralized health care fraud database of final adverse actions. These officials cited the benefit of having access to background information about providers and practitioners in a single location, which would make the early stages of an investigation more efficient. Moreover, GAO's survey of insurance commissioners found that almost all of the respondents who investigated health care fraud during 1994 favored a database of final adverse actions. While supporting the concept of a final adverse actions database, however, many of the other officials GAO interviewed believed it would not be an essential element of an effective anti-fraud enforcement effort but might provide some investigative benefits. In addition, almost all of these officials expressed concerns about maintaining security over the information in the database, as well as the possibility that the information in the database would be misused.

As an alternative to final adverse actions, many officials GAO interviewed suggested that information about ongoing health care fraud investigations and reports of suspected fraud would be useful to include in a centralized database. Officials at 13 of the 31 offices supported a database with ongoing investigative information, saying, for example, it could help eliminate investigative duplication by identifying multiple agencies investigating the same subject. Officials at eight offices supported a database containing reports of suspected fraud, with one official saying that a suspected fraud database would allow government investigators to better identify fraudulent schemes involving multiple insurers. The officials noted that these alternatives would pose more risks than a database of final adverse actions (which consists of publicly available information), due to the sensitivity of the information and the resulting need for security to prevent inappropriate disclosure and possible misuse.

In addition to the risks posed by inappropriate disclosure or misuse of information in the database, the establishment of a centralized database also involves uncertainties about development and operating costs that have not been addressed. GAO identified a large, federally funded, adverse actions database—the National Practitioner Data Bank—which, although it does not deal specifically with health care fraud and is not used by law enforcement agencies, might serve to illustrate the cost of a health care

fraud database. Containing over 97,000 records and receiving over 1 million inquiries annually, the Data Bank has cost about $24 million to establish and operate over the past 7 years.

Recommendations

GAO is making no recommendations in this report.

Comments

GAO solicited comments on a draft of this report from the Department of Justice, NHCAA, and the American Medical Association. Justice provided technical and clarifying comments, which GAO incorporated where appropriate. NHCAA and the American Medical Association provided written comments, which are presented and evaluated in chapters 2 and 3. NHCAA said that it strongly supports the adoption of an effective federal immunity statute and believes that such a statute is needed to adequately protect private payers that participate in multistate fraud investigations. Also, NHCAA commented that a centralized database, if properly created with complete information and appropriate access for public and private payers, could be an excellent supplemental tool for fighting health care fraud. The American Medical Association said that it supports granting immunity to those reporting incidents of health care fraud, provided adequate safeguards are established so that the nature of the conduct reported is specific, physician's medical decisions are not grounds for accusations of fraud, and there is legal recourse for "bad faith" reporting. On the other hand, the Association also said that a centralized database may not be the best use of limited enforcement resources and that there are many problems inherent in establishing and maintaining such a database.

Contents

Executive Summary		2
Chapter 1 Introduction		12
	Size and Complexity of Health Care System Complicates Enforcement Efforts	13
	Information Sharing Is Critical to Effective Enforcement Efforts	18
	Objectives, Scope, and Methodology	19
Chapter 2 Concept of Expanded Federal Immunity Law With Appropriate Safeguards Is Broadly Supported		24
	Immunity Protects Persons Who Report Suspected Fraud	24
	Current Federal Immunity Law Is Limited in Its Scope	26
	State Laws Reflect a Range of Immunity Provisions Related to Insurance Fraud	27
	Recent Proposals Would Enhance Immunity Protection Provided by Federal Law	28
	Industry and Law Enforcement Officials Generally Favor Broad Federal Immunity Legislation With Appropriate Safeguards	30
	Conclusions	39
	Comments and Our Evaluation	40
Chapter 3 Centralized Health Care Fraud Database May Be Beneficial but Some Questions Remain		41
	Databases and Other Information Resources Useful to Health Care Fraud Investigators	41
	Recent Proposals Would Create a National Database of Health Care Fraud-Related Information	44
	Law Enforcement and Industry Have Mixed Views on the Benefits of a Centralized Health Care Fraud Database	48
	Conclusions	56
	Comments and Our Evaluation	56
Appendixes		
	Appendix I: Organizations Contacted by GAO	58
	Appendix II: Comparison of State Immunity Statutes	60
	Appendix III: State Insurance Commissioners Health Care Fraud Survey	64
	Appendix IV: Databases and Other Information Resources That May Be Useful to Health Care Fraud Investigators	79
	Appendix V: Comments From the National Health Care Anti-Fraud Association	86
	Appendix VI: Comments From the American Medical Association	92
	Appendix VII: Major Contributors to This Report	96

Tables

Table 3.1: Recent Proposals to Create a National Database of Health Care Fraud-Related Information 45
Table I.1: Federal and State Agencies and Private Insurers Contacted in Four States 58
Table I.2: National Insurance Companies Contacted in Connecticut and Illinois 58

Figure

Figure 1.1: Illustration of the Complex Health Care Fraud Enforcement Environment 17

Abbreviations

DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
HHS	Department of Health and Human Services
NHCAA	National Health Care Anti-Fraud Association

Introduction

The size of the health care sector and sheer volume of money involved make it an attractive target for fraud. Expected to total over $1 trillion in fiscal year 1995, health care spending will consume almost 15 percent of the gross national product, an increase from just over 12 percent in 1990. The amount of fraud within the health care system is, by its nature, impossible to accurately determine. We have previously reported[1] that 10 percent of all health care expenditures may be lost to fraud and abuse.[2] Similarly, industry estimates have placed the annual losses due solely to fraud at somewhere between 3 and 10 percent of all health care expenditures (between $30 billion and $100 billion based on estimated fiscal 1995 expenditures).[3] By whatever estimate, this represents a significant monetary drain on our health care system.

Health care fraud can take many forms, reach all facets of the industry, and be perpetrated by persons both within and outside the health care industry. A recent report by the Federal Bureau of Investigation (FBI), for example, notes that vulnerabilities to fraud exist throughout the entire health care system, and patterns of fraud are so pervasive that systemic criminal activity is accepted as a "way of doing business" in many segments of the health care industry.[4] A 1995 Department of Justice (DOJ) report on health care fraud[5] states that fraud is being perpetrated not only by individual physicians, but also by public corporations, medical equipment dealers, laboratories, hospitals, nursing homes, and individuals who provide no health care at all but prey upon the system with fraudulent scams. As the DOJ report goes on to note, everyone pays the price for health care fraud, as reflected by higher insurance premiums, increased costs for medical services and equipment, and greater expenditures for Medicare and other public health care programs.

Successful health care fraud prosecutions illustrate the types of fraudulent activities taking place. Ranging from simple schemes to complex conspiracies, some frauds have even put lives at risk. As described in the

[1]Health Insurance: Vulnerable Payers Lose Billions to Fraud and Abuse (GAO/HRD-92-69, May 7, 1992).

[2]Both fraud and abuse result in inappropriate expenditures. Fraud generally involves a willful or knowing act, while abuse involves actions that are inconsistent with acceptable business and medical practices.

[3]Testimony of William J. Mahon, Executive Director, National Health Care Anti-Fraud Association, before the House Subcommittee on Crime and Criminal Justice, Committee on the Judiciary, July 19, 1994.

[4]Health Care Fraud: Medical Fraud and Legislative Remedies, Federal Bureau of Investigation. December 1994.

[5]Department of Justice Health Care Fraud Report, Fiscal Year 1994. March 2, 1995.

1995 DOJ report, examples of fraudulent activities that have been federally prosecuted include the following:

- An optometrist defrauded Medicare and private insurance companies of over $1.5 million simply by billing for services that were unnecessary or not rendered.
- A husband and wife set up a fraudulent network of offshore corporations and entities, which they used to defraud a private insurance company as well as employer insurance networks in several states. This scheme left policyholders with approximately $6 million in unpaid medical and reinsurance claims.
- A medical supplier fraudulently submitted false statements to the Food and Drug Administration about the efficacy of heart catheters. Three persons died, and 22 others required emergency heart bypass surgery when these devices were distributed to hospitals and physicians.

We have previously reported that several serious fraud problems are facing public and private payers.[6] First, large financial losses to the health care system can occur as a result of even a single scheme. Second, fraudulent providers can bill insurers with relative ease. Third, efforts to prosecute and recover losses from those involved in the schemes are costly; even convictions often do not result in the recovery of losses. Finally, fraudulent schemes can be quickly replicated throughout the health care system. Moreover, as discussed below, a multiplicity of health care payers—each with its own operating policies and subject to various enforcement agencies—further complicates health care fraud enforcement efforts.

Size and Complexity of Health Care System Complicates Enforcement Efforts

Of the estimated $884 billion spent on health care in 1993, about 44 percent was paid with public sector dollars, and 56 percent was paid with private sector dollars. Federal health insurance programs—such as Medicare, Medicaid, the Veterans Health Administration, the Federal Employees' Health Benefit Program, and the Civilian Health and Medical Program of the Uniformed Services—collectively accounted for almost three-quarters of all public health care expenditures. Private health insurance—which includes the various Blue Cross/Blue Shield plans, a host of other private health insurance companies, and many employers

[6]Health Insurance: Legal and Resource Constraints Complicate Efforts to Curb Fraud and Abuse (GAO/T-HRD-93-3, Feb. 4, 1993); and Health Insurance: Vulnerable Payers Lose Billions to Fraud and Abuse (GAO/HRD-92-69, May 7, 1992).

who self-insure—accounted for about 60 percent of all private sector expenditures.[7]

Public and private payers in the current health care system number over 1,000. Generally, each payer has its own system of processing health care claims and reimbursing providers. Payers may have different rules, reimbursement policies, claim forms, multiple identification numbers, coding systems, and billing procedures. When combined with the sheer size of the health care industry—an estimated 4 billion health claims are processed annually—this complex system of payers presents considerable challenges for those organizations responsible for detecting and pursuing health care fraud.

Within this complex system, various federal enforcement agencies have responsibility for investigating health care fraud. For example, the Department of Health and Human Services (HHS) Office of Inspector General has primary responsibility for the Medicare and Medicaid programs, the Department of Veterans Affairs Office of Inspector General has primary responsibility for the Veterans Health Administration, the Department of Defense Criminal Investigative Service has primary responsibility for the Civilian Health and Medical Program of the Uniformed Services, and the Office of Personnel Management Office of Inspector General has primary responsibility for the Federal Employees' Health Benefits Program. The FBI and the U.S. Postal Inspection Service, under existing federal criminal statutes, have broader authority to investigate fraud in any public or private program.[8] Other agencies that are involved in health care fraud enforcement include the Drug Enforcement Administration, Internal Revenue Service, and Department of Labor.

In addition to federal enforcement agencies, states also have health care fraud enforcement responsibility. Regarding Medicaid, for example, while HHS is responsible for oversight of the program, the agency has largely delegated primary investigative enforcement responsibility to state

[7]The remaining private sector expenditures were out-of-pocket consumer expenditures (32 percent), including deductibles and co-insurance required by public and private insurers; and nonconsumer expenditures (8 percent), such as research and construction.

[8]Excepting Medicare and Medicaid, there is no specific federal health care fraud criminal or civil statute. Therefore, criminal fraud affecting other public or private health programs is typically investigated under general federal criminal statutes. Since most fraudulent schemes involve use of the mail, the mail fraud statute (18 U.S.C. 1341) is the most commonly used federal criminal authority. In the civil area, most health care fraud cases are brought as violations of the False Claims Act, 31 U.S.C. Sec. 3729, et seq.

Medicaid Fraud Control Units,[9] which are predominately funded through federal grants. Regarding private insurance, some states have established insurance fraud bureaus that investigate health care fraud; in other states, the department of insurance has a fraud unit that investigates fraud. While these state agencies can often pursue administrative and civil penalties for health care fraud, most criminal enforcement authority is in the hands of local prosecutors and attorneys general.

The private sector is also active in health care fraud enforcement. Private insurers have established active anti-fraud programs and special investigative units that work with a wide range of public law enforcement agencies to investigate fraud. These units may report fraud cases to federal or state agencies with health care fraud enforcement responsibility. In addition, a group of private sector health insurers and public sector law enforcement agencies has established the National Health Care Anti-Fraud Association (NHCAA), which represents a cooperative effort to prevent health care fraud and improve capabilities to detect, investigate, and prosecute such fraud.[10] The NHCAA conducts anti-fraud education seminars, provides a forum for members to share information on fraudulent schemes, and assists law enforcement in the investigation and prosecution of health care fraud.

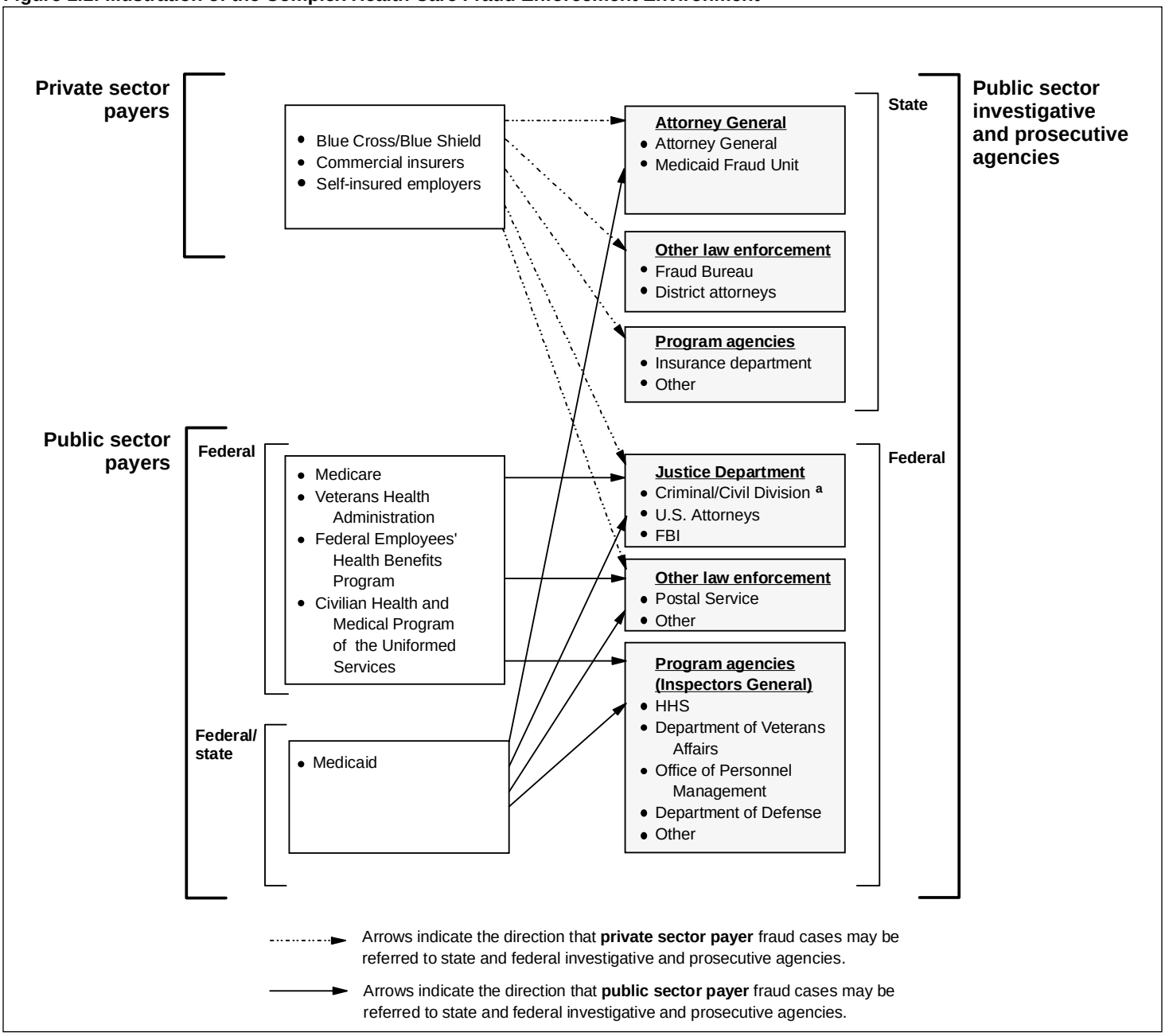
As shown in figure 1.1, while public sector health care fraud is primarily the responsibility of federal enforcement and program agencies, private sector fraud can be pursued by both state and federal enforcement agencies. In some states, private insurers are required by law to report suspected fraud to state enforcement agencies, while reports to federal enforcement agencies are optional at the discretion of the insurer. In addition to the reporting of suspected fraud from insurers to federal and state authorities, fraud-related information can also be shared between federal and state authorities. In commenting on a draft of this report, DOJ

[9]The Omnibus Budget Reconciliation Act of 1993 required all states to establish a Medicaid Fraud Control Unit by January 1995, unless a state can show that a fraud unit would not be cost effective because there is minimal Medicaid fraud in the state. As of January 1996, 47 states had active Medicaid Fraud Control Units.

[10]Founded in 1985, NHCAA's membership includes 70 private sector corporate members, as well as public sector participants from the Offices of Inspector General at the U.S. Departments of Defense, HHS, Labor, and Veterans Affairs and at the Office of Personnel Management; the Health Care Financing Administration; the criminal investigation division of the U.S. Postal Inspection Service; and the National Association of Medicaid Fraud Control Units. NHCAA also maintains formal "law enforcement liaison" relationships with DOJ, FBI, the Federal Trade Commission's Bureau of Consumer Affairs, and the Internal Revenue Service's Criminal Investigation Division. NHCAA also numbers more than 800 individual members from the ranks of these private and public sector organizations and from other health insurance companies, self-insured corporations, and federal and state agencies. In 1993, NHCAA member insurers represented an estimated $110 billion in direct health benefits paid.

officials told us that the Department has placed increasing emphasis on working with the Medicaid Fraud Control Units and NHCAA.

Figure 1.1: Illustration of the Complex Health Care Fraud Enforcement Environment



[a]In addition to criminal prosecutions (which may involve public or private insurer fraud), the Justice Department also pursues civil enforcement actions, particularly where federal health insurance programs have been defrauded.

Source: Developed by GAO on the basis of contacts with applicable organizations (see app. I).

Information Sharing Is Critical to Effective Enforcement Efforts

Federal law enforcement officials have characterized health care fraud investigations as some of the most complex of all white-collar crime cases. Over the years, however, the scope and complexity of health care fraud has changed. In 1994, for example, HHS reported that:

"In the 1970s, we found that we were largely dealing with individual providers who were involved in relatively uncomplicated schemes, such as filing false claims which resulted in a few thousand dollars of damage to the Medicare program. Today, it is more common to see cases involving groups of people who defraud the Government. Some of the schemes are relatively complex, often involving the use of sophisticated computer techniques, complicated business arrangements, and multiple locations across state lines. These crimes can cause losses in the tens of millions of dollars to Medicare and Medicaid, as well as to other public and private health insurance programs."[11]

Along with the increasing complexity of health care fraud, law enforcement and regulatory agencies and insurers have recognized the importance of coordinating their enforcement efforts and exploring methods for sharing health care fraud information. A health care reform bill introduced before the U.S. Senate in November of 1993 identified a "national need" to coordinate health care fraud-related information and went on to state that control of fraud and abuse in health care services warrants greater efforts of coordination than those that can be undertaken by individual states or the various federal, state, and local law enforcement programs.[12]

A coordinated enforcement effort has to involve not only public law enforcement agencies, but also the private sector. Given their position of having daily interaction with health providers, private insurers often possess more information about a provider's activities than state and federal agencies. This position, coupled with their own incentive to reduce costs, has made insurers another source of information for government investigators and prosecutors.

Because many insurers have established special investigative units that pursue fraud, these private sector resources can be used to leverage

[11]Testimony of Michael Mangano, Principal Deputy Inspector General, HHS, before the Senate Committee on the Judiciary, May 25, 1994.

[12]S. 1770, "Health Equity and Access Reform Today Act of 1993," Title IV, Section 4121; introduced by Senator John Chafee on November 22, 1993.

existing public sector investigative resources. The insurance industry has developed sophisticated methods for detecting fraud, and development of contacts with the industry can provide a valuable source of fraud case referrals to the federal government. For example, the FBI recently reported that on the basis of fraud referrals by several private insurance company investigative units, government investigators were able to identify a medical billing company that defrauded $1.5 million from insurance companies across the country.[13] Moreover, because fraudulent schemes often target public and private programs simultaneously, an active anti-fraud enforcement effort involving private insurers may lead to the discovery of additional fraud involving public sector health programs.

In recent years, there have been various proposals designed to enhance information sharing among federal, state, and private entities involved in health care fraud enforcement. Some proposals, for example, have called for federal immunity legislation to provide protection for persons who report suspected fraud. The purpose of such immunity laws is to encourage insurers and private individuals to report suspected fraud to law enforcement agencies by protecting the individuals from subsequent civil actions. Other proposals have called for establishment of a national, centralized database of health care fraud-related information. The purpose of a centralized database would be to provide public and private sector fraud investigators with easy access to information about health care fraud activity nationwide and to enhance coordination of investigative efforts among insurers and law enforcement agencies.[14]

Objectives, Scope, and Methodology

In an October 6, 1993, letter, the former Chairman of the House Subcommittee on Information, Justice, Transportation, and Agriculture, Committee on Government Operations,[15] asked us to broadly examine

[13]Testimony of Thomas T. Kubic, Chief, Financial Crimes Section, Criminal Investigative Division, FBI, before the House Subcommittee on Crime and Criminal Justice, Committee on the Judiciary, July 19, 1994.

[14]For more detail on the immunity and centralized database issues, see chapters 2 and 3, respectively.

[15]During the 104th Congress, this Subcommittee was abolished. Jurisdiction for this request passed to the Ranking Minority Member of the newly established Subcommittee on National Security, International Affairs and Criminal Justice, Committee on Government Reform and Oversight.

health care fraud enforcement issues. On the basis of this request and subsequent discussions with the new Subcommittee's Ranking Minority Member, we agreed to focus our work on questions about information-sharing issues that may affect health care fraud enforcement efforts, specifically:

- What is the extent of federal and state immunity laws protecting persons who report health care fraud-related information (see ch. 2)?
- What evidence exists for and against establishing a centralized health care fraud database to enhance information sharing and support enforcement efforts (see ch. 3)?

Literature Review

To address these two questions, we first reviewed relevant literature to obtain a broad understanding of the importance of information sharing in anti-fraud enforcement efforts. This literature included reports issued by government and private sector organizations—such as DOJ, HHS, and NHCAA—that are responsible for managing and/or overseeing health care anti-fraud activities. We also reviewed the provisions of relevant proposals presented in recent years by administration and congressional sponsors that would enhance information sharing among the various federal, state, and private entities responsible for health care fraud enforcement. These included a 1992 proposal by the Bush administration, as well as proposals introduced in House and Senate bills during 1993 and 1995, respectively.

National Perspectives

To obtain a broad understanding of both the immunity and the centralized database issues, we contacted key governmental and private organizations that could provide nationwide perspectives. Federal government contacts included officials at DOJ, FBI, the U.S. Postal Inspection Service, and the Executive Office for U.S. Attorneys, as well as Office of Inspector General officials at the principal agencies responsible for managing major federal health care programs—HHS, the Office of Personnel Management, and the Department of Defense. Private sector contacts—representing industry, professional, and special interest organizations—included the American Medical Association, the Health Insurance Association of America, the National Insurance Crime Bureau, and NHCAA.[16] In meetings with knowledgeable officials at several of these governmental and private organizations, we also obtained perspectives on S. 1088 (the Health Care

[16]The American Medical Association represents physicians, residents, and medical students; the Health Insurance Association of America represents companies that write and sell health insurance. Both Associations provide member services, as well as monitor legislation and regulations affecting their membership. The National Insurance Crime Bureau is discussed in more detail in appendix IV.

Fraud and Abuse Prevention Act of 1995),[17] which contains immunity and centralized database provisions and was pending further congressional consideration at the time of our review.

State Selection and Visits

To obtain additional perspectives on the immunity and centralized database issues, we contacted relevant public and private sector officials in four states—Florida, Maryland, Massachusetts, and Texas (see app. I). In judgmentally choosing these four states, we considered various factors, including (1) the status or scope of the state's immunity law, (2) the extent of anti-fraud activities undertaken by applicable enforcement agencies, and (3) selection suggestions made to us by law enforcement officials and insurance industry organizations. To the extent practical with just four states, we wanted the selections to reflect a range of immunity and/or anti-fraud enforcement environments. For example, at the time we made the selections:

- Maryland had no state immunity law protecting persons who reported suspected health care fraud, while Massachusetts' immunity law protected only reports made to the state fraud bureau. Florida and Texas both had broader immunity laws that protected disclosures made to both federal and state agencies.[18]
- Florida and Texas both had state fraud units within the Department of Insurance; Maryland and Massachusetts had independent or stand-alone fraud bureaus.[19] Further, an FBI official told us that FBI field offices in these four states were among the most active in private sector health care fraud investigations.

In visiting each state, we met with officials from various federal and state prosecutive, investigative, and regulatory agencies—U.S. Attorneys offices, FBI and U.S. Postal Inspection Service field offices, state departments of insurance and fraud bureaus, and state attorneys general. We also met with general counsel and special investigative unit officials at selected private insurance companies in these four states. As appendix I shows, our total number of contacts in these 4 states included 12 federal offices, 6 state offices, and 8 private insurance companies. To obtain

[17]This bill was originally introduced in January 1995 as S. 245 and was superseded by S. 1088 in July 1995. Both bills contained essentially identical immunity and centralized database provisions.

[18]During 1995, both Florida and Texas expanded their immunity laws to protect the sharing of fraud-related information between insurance companies, and Maryland enacted a state immunity law. Our field work focused on conditions before these laws took effect.

[19]During 1995, Maryland's fraud bureau was placed under the authority of the state insurance department.

additional insurance company perspectives, we also visited five national insurers at their headquarters located in Connecticut and Illinois, respectively. Thus, in total, we visited 13 private insurance companies.[20]

At each organization visited, we interviewed those officials responsible for anti-fraud enforcement efforts. Regarding the immunity issue, we obtained information and views about (1) how fraud-related information is being shared between investigative and prosecutive entities, (2) what impact immunity laws (or the absence of such laws) have had on the willingness of individuals to report suspected fraud, and (3) whether a federal immunity law is needed to enhance information sharing. Regarding the centralized database issue, we obtained information about (1) how computerized databases are being used in investigating fraud; (2) whether a national, centralized database is needed to enhance enforcement efforts; and (3) what factors should be considered in establishing such a database. Our direct observations about health care fraud enforcement issues are limited to the locations visited and may not reflect circumstances or conditions in other locations.

Survey of State Insurance Commissioners

To obtain information on the immunity and centralized database issues from state officials responsible for insurance regulation, we mailed a questionnaire to all 50 state insurance commissioners (or to an equivalent state insurance regulatory official). We developed and pretested the questionnaire with input from officials with the National Association of Insurance Commissioners and an official with the survey population. We mailed the questionnaire in July 1995, and we received responses from all 50 states between July and November 1995. A copy of the questionnaire, with a tabulation of responses to each applicable question, is presented in appendix III.

Although we surveyed and received responses from the population of state insurance commissioners, the practical difficulties of conducting any survey may, nonetheless, introduce unintended nonsampling errors. For example, variations in the wording of questions or the sources of information available to the respondents can introduce variability into the survey results. However, as noted above, in order to minimize these errors, we pretested our survey. Also, all survey data were verified during data

[20]We judgmentally selected and visited insurance companies suggested to us by various industry or regulatory organizations, including NHCAA, the Health Insurance Association of America, and the National Association of Insurance Commissioners. The selections were based, in part, upon the availability and/or willingness of company officials to meet with us.

entry and all computer analyses were reviewed by a second independent analyst.

We did our work from September 1994 through December 1995 in accordance with generally accepted government auditing standards. NHCAA and the American Medical Association provided written comments on a draft of this report. These comments are included in appendixes V and VI and are summarized and evaluated at the end of chapters 2 and 3. DOJ provided technical and clarifying comments, which we incorporated where appropriate in this report.

Concept of Expanded Federal Immunity Law With Appropriate Safeguards Is Broadly Supported

The purpose of immunity statutes is to encourage insurers and private individuals to report suspected fraud by protecting them from civil claims subsequently arising from insurance fraud investigations. We identified no federal law that protects persons providing health care fraud-related information to law enforcement agencies. However, there are some related immunity provisions on the federal level. Regarding Medicare and Medicaid, for example, current federal statutory law providing immunity from liability is limited to persons reporting information to peer review contractors about Medicare and Medicaid health care services. This immunity protection is further limited in that it does not apply to persons reporting fraud-related information to federal authorities, such as HHS, the FBI, and the U.S. Postal Inspection Service. It also does not apply to persons who report suspected health care fraud involving private sector insurance, even if the suspected fraud is reported to a federal agency. While most states have enacted immunity laws that protect persons who report suspected health care fraud more broadly than current federal law, the laws vary considerably. For example, some state laws protect sharing of suspected fraud information with any federal or state law enforcement authority, whereas some states protect information sharing only with certain state authorities.

In recent years, various health care anti-fraud proposals (some included in health care reform bills) have been introduced by the administration and Congress to, among other matters, provide a broader federal immunity statute. The health care reform bills were not enacted, however, and at the time of our review, one health care anti-fraud bill (S. 1088)—which was awaiting congressional consideration—would provide immunity protection more broadly than current federal law. The health insurance and medical industry associations we contacted supported the concept of a federal immunity law. Additionally, nearly two-thirds of the federal and state government fraud investigators and prosecutors and 12 of 13 insurance company representatives we interviewed supported a federal immunity law. In fact, many of the individuals we spoke with thought that federal immunity protection should be broader than the immunity proposed under S. 1088.

Immunity Protects Persons Who Report Suspected Fraud

Broadly viewed, public policy supports both encouraging private entities to participate in the investigation and prosecution of fraud and providing protection to innocent people against unsubstantiated allegations made in bad faith or with malice. That is, given the public interest in crime prevention, reasonable private participation in the investigation and

prosecution of crime is a desirable objective. Immunity statutes are one way of encouraging this objective. On the other hand, concerns have been raised about the need to incorporate safeguards to provide individuals with protection against bad faith allegations. Safeguards that have been considered include requirements governing the specificity and credibility of reported information and provisions giving individuals legal recourse against bad faith allegations that could seriously damage an individual's life and livelihood if publicly disclosed.

Immunity statutes represent part of the general public policy to encourage private involvement in the prosecution of crime by protecting persons against civil claims subsequently arising from insurance fraud investigations. For instance, the reporting of an individual suspected of fraud may result in the named, suspected party filing a civil suit against the reporter claiming defamation of character.[1] Immunity statutes typically include limiting language, such as "in the absence of malice or bad faith," which allows an individual claiming defamation the opportunity to show that the reporting party intended to harm the individual. However, where there is an applicable immunity statute and the individual claiming defamation is not able to show malice or bad faith, the reporting party is provided protection from these types of lawsuits.

It is important to note that a number of civil claims can be raised against insurers stemming from fraud investigations and, in most cases, there is no way to prevent an aggrieved party from filing a civil lawsuit against an individual who reports suspected fraud. An immunity statute does, however, make it more difficult for a claimant to prevail. For example, in a 1992 civil action in Ohio,[2] an individual brought action for damages against a health insurer for reporting suspected fraud to the state insurance department. The focus of the case was whether the plaintiff could recover from the insurer for defamation. The federal district court held that the insurer faced no civil liability for reporting suspected fraud because Ohio law provides immunity to persons who furnish information—in good faith and without malice or fraud—to the Ohio Department of Insurance.[3] Since the court found nothing in the record suggesting bad faith, the insurer prevailed in its motion for summary judgment.

[1]"Defamation" is defined as an intentionally false communication, either written or spoken, that injures someone's reputation or good name.

[2]Mann v. American Packaging Corporation, 809 F. Supp. 32 (S.D. Ohio 1992).

[3]Ohio Revised Code section 3999.31(B) provides immunity, in the absence of fraud or bad faith, for any person providing information concerning insurance fraud to the state's Division of Insurance Fraud or Department of Insurance.

Current Federal Immunity Law Is Limited in Its Scope

We found no immunity provision on the federal level designed to protect persons who report suspected health care fraud to law enforcement agencies. However, with respect to the Medicare and Medicaid programs, section 1157 of the Social Security Act, as amended (codified at 42 U.S.C. 1320c-6(a)), would provide immunity, under certain circumstances, to persons who report health care fraud-related information. This law specifically states the following:

"Notwithstanding any other provision of law, no person providing information to any [peer review] organization having a contract with the Secretary [of HHS] under this part shall be held, by reason of having provided such information, to have violated any criminal law, or to be civilly liable under any law of the United States or of any State (or political subdivision thereof) unless—(1) such information is unrelated to the performance of the contract of such organization; or (2) such information is false and the person providing it knew, or had reason to believe, that such information was false."

Our review did not identify any similar federal statutory immunity provisions applicable to other government health care programs, such as the Federal Employees' Health Benefits Program (managed by the Office of Personnel Management) and the Civilian Health and Medical Program of the Uniformed Services.[4]

As indicated, the Medicare/Medicaid statute specifically protects only information disclosures made to a peer review organization under contract with the Secretary of HHS. Under federal law, the Secretary enters into contracts with peer review organizations for the purpose of promoting the effective, efficient, and economical delivery of quality health care services under Medicare. Composed primarily of health care practitioners from within a geographical area, these organizations perform quality assurance and utilization reviews of health care providers seeking reimbursement for their Medicare services. If a peer review organization determines that a practitioner or provider has persisted in violating his obligation to provide services that (1) are medically necessary, (2) meet professionally recognized standards of care, and (3) are cost-effective, the reviewer may recommend that the practitioner or provider be excluded from the Medicare program. In addition, states can also choose to use peer review organizations to review care received by Medicaid patients.

Even in reference to the HHS-managed Medicare and Medicaid programs, this federal statutory immunity provision is limited. For instance, the

[4]In commenting on a draft of this report, DOJ officials noted that the whistleblower provisions of 31 U.S.C. Sec. 3730(h), while limited in scope, may provide a defense in certain civil suits.

immunity protection does not cover reporting directly to any federal law enforcement authority. Thus, an individual who reports suspected Medicare fraud directly to the HHS Office of Inspector General—or to other federal authorities, such as the FBI and the U.S. Postal Inspection Service—would not be provided immunity protection under 42 U.S.C. 1320c-6(a). DOJ, however, would ordinarily defend Medicare contractors or their employees who are sued in connection with Medicare anti-fraud efforts. In a July 1995 letter to Medicare contractors, DOJ and the Health Care Financing Administration noted:

> "We believe that Medicare contractors who are carrying out official functions related to administration of the Medicare program, particularly those who are engaged in efforts to detect, prevent, or prosecute program fraud and abuse, should be entitled to protections similar to those enjoyed by Federal employees engaged in those activities. For that reason, the Department of Health and Human Services will ordinarily request, and the Department of Justice will ordinarily agree, that the Department of Justice will defend, at its own expense, any Medicare contractor or employee of a contractor, who is sued in connection with activities undertaken within the scope of the Medicare contract."

Further, the federal statutory immunity provision does not protect persons who report suspected fraud involving private sector insurance plans, even if the suspected fraud is reported to a federal agency such as the FBI or the U.S. Postal Inspection Service. Existing state immunity laws would provide some statutory immunity protection under these circumstances.

State Laws Reflect a Range of Immunity Provisions Related to Insurance Fraud

Many states have enacted immunity laws to protect individuals who report suspected insurance fraud—including health care fraud. The responses to our survey of the 50 state insurance commissioners indicate that state immunity laws vary considerably in terms of protection provided to private insurers who disclose fraud-related information.[5] As appendix II shows, at the time of our survey, 38 states had enacted immunity laws protecting the sharing of health care fraud-related information, while 12 states had no immunity laws applicable to health care fraud. In the 38 states with immunity laws, typically only specific reporting channels are covered. For example, 24 states provide immunity to insurers for sharing fraud-related information with state and federal law enforcement authorities, as well as with the state insurance commissioner. However, 10 states provide immunity for sharing fraud-related information only with the state insurance commissioner. Eight states provide immunity to

[5]See appendix II for a comparison of state immunity statutes and appendix III for a copy of the survey questionnaire.

insurers for sharing fraud-related information with other insurers. All 38 states with immunity laws place certain qualifications on the provision of immunity. In each of these states, for instance, the immunity is contingent on the absence of "bad faith" or "malice." However, the meaning of these qualifications and the ultimate protection provided under the law are subject to interpretation by individual court systems.

Much like existing federal immunity law, state immunity laws are also limited in the level of protection they provide. Due to variances in state laws, the immunity protection provided can be different from state to state. These differences can present concerns for private insurers that operate nationally, especially if a suspected fraudulent scheme involves more than one state. An insurer investigating a multistate fraud scheme, for example, may have concerns about which state's immunity law applies to the sharing of case information. Also, as discussed above, 12 states have no immunity laws applicable to health care fraud. Anyone reporting suspected private insurer fraud in these states has no specific statutory protection from subsequent civil lawsuits.

Recent Proposals Would Enhance Immunity Protection Provided by Federal Law

In recent years, federal proposals have been introduced that would broaden existing immunity protection. Ranging from a 1993 executive branch task force proposal to a 1995 anti-fraud bill currently awaiting consideration by Congress, these proposals would provide some federal immunity protection to persons who report suspected health care fraud—regardless of whether the fraud involves public or private payers within the health care system.

In 1993, to enhance health care fraud enforcement efforts, a Bush administration task force[6] recommended, among other things, providing immunity for reporting information to a national database, which the task force also recommended be created.[7] Immunity from both federal and state claims would have been provided to database participants reporting fraud-related information to (or obtaining such information from) this database in good faith. Also, the proposed immunity provision contained a requirement that any complainant alleging malice or bad faith must plead with specificity the facts that constitute malice or bad faith in order to invoke an exception to immunity. The recommendations of the task force

[6]The Bush Administration Task Force to Combat Health Care Fraud and Abuse consisted of personnel from DOJ, HHS, and the Office of Management and Budget.

[7]The proposed database, as discussed further in chapter 3, was to contain information relating to ongoing health care fraud investigations.

were not adopted, although, as noted below, the immunity proposal was reintroduced in subsequent congressional legislation.

During 1993 and 1994, some form of federal immunity provision was included in various health reform bills introduced in Congress. In November 1993, for example, the Clinton administration introduced H.R. 3600 (the "Health Security Act"), which would have established federal immunity for reporting suspected health care fraud to HHS and DOJ. Because the proposed Health Security Act would have created a national framework for the delivery of health care, this immunity provision would have applied to the reporting of any suspected health care fraud throughout the health care system. By late summer 1994, the original Clinton reform bill had been essentially dropped by both the House and the Senate. Neither the Health Security Act nor any of the other health reform bills were enacted.

In July 1995, Senator William Cohen introduced S. 1088 (the "Health Care Fraud and Abuse Prevention Act of 1995"), which contains various provisions designed to enhance anti-fraud enforcement efforts. One of the bill's provisions would extend the protection provided in 42 U.S.C. 1320c-6(a) to include persons providing information about any public or private health plan to either HHS or DOJ.[8] This expansion would address some of the limitations of current federal law. For example, a person reporting suspected Medicare fraud to HHS and a person reporting private insurance fraud to DOJ would be protected under this bill. Further, the bill's immunity provision would provide some statutory protection in the 12 states that have no immunity law and also may provide, in those states with immunity laws, an additional channel for reporting suspected fraud.

Although S. 1088 would provide immunity protection more broadly than current law, the provision does not address the role of all entities involved in anti-fraud enforcement. For example, under S. 1088, immunity protection would not be provided to persons who report fraud information to law enforcement entities other than DOJ and HHS. The proposal does not address the role of other federal agencies (such as the U.S. Postal Inspection Service) and state agencies (such as Attorneys General and state fraud bureaus) that also conduct health care fraud investigations. Also, the proposal does not address sharing from one insurer to another, a provision already included in some state immunity laws. One recent federal anti-fraud proposal does address insurer-to-insurer information

[8]This immunity provision was originally introduced by Senator Cohen in S. 245 (the "Health Care Fraud Prevention Act of 1995") and was later incorporated into S. 1088.

sharing. H.R. 2408, introduced September 27, 1995, would extend the provisions of 42 U.S.C. 1320c-6(a) to provide immunity for, among other things, "health plans sharing information in good faith and without malice with any other health plan with respect to matters relating to health care fraud detection, investigation and prosecution."

Industry and Law Enforcement Officials Generally Favor Broad Federal Immunity Legislation With Appropriate Safeguards

Industry organizations, such as NHCAA and the Health Insurance Association of America, have stated that due to the potential for civil lawsuits, private insurers are concerned about sharing fraud-related information with law enforcement agencies. These industry organizations contend that a federal immunity law would facilitate the flow of information between insurers and law enforcement agencies and enhance investigation and prosecution of health care fraud cases. This contention includes a general recognition of the need for appropriate safeguards against bad faith allegations. Medical associations also told us they generally support immunity protection for individuals who report suspected fraud. Most of the investigative and prosecutive officials we interviewed—which included investigators and prosecutors at federal and state agencies and special investigative unit personnel at various insurance companies—also told us that a federal immunity law would enhance health care anti-fraud enforcement efforts.

National Health Care Anti-Fraud Association

In August 1993, the NHCAA Board of Governors adopted a policy option calling for preemptive federal legislation to provide uniform immunity protection across all states:

"The need for a concerted anti-fraud effort involving the sharing of information among private payers and with law enforcement is being widely acknowledged. However, while many states provide some immunity protection for those engaging in good faith fraud investigations, this protection varies tremendously by state; many states have no immunity statute. . . . This piecemeal state legislation simply does not protect insurers and other payers in many states or in multi-state investigations.

"Therefore Congress should consider enacting an immunity statute that would immunize payers' good-faith efforts to fight fraud and provide immunity from state tort liability. Such a statute would preempt the inconsistent, vague and often ill-considered state law jeopardy faced by insurers and other payers . . . and would create a standardized and effective tool to encourage fraud fighting.

"Like many state statutes, this immunity protection would not be absolute, and reasonably would be limited to those investigations conducted with good faith or the absence of malice. However, to make this protection effective, Congress should consider the addition of a provision, modeled on Rule 9(b) of the Federal Rules of Civil Procedure, that requires a person to plead with specificity the facts that constitute malice or bad faith in order to invoke this exception to immunity."[9]

In 1993 testimony before Congress, the NHCAA Executive Director stated that before forwarding a case for investigation and prosecution, insurers always have to consider the probability of lawsuits for defamation, slander, and malicious prosecution, and that these lawsuits, even if they are completely without merit, are at best very costly to the insurer.[10] During our review, the NHCAA Executive Director told us that encouraging insurers to report fraud is important because the extent of health care fraud is increasing. He noted that, historically, insurers would simply write off fraud and pass the losses on to policyholders because fraud was not deemed to be that significant a problem. He added that some insurers saw no alternative to such write-offs because health care fraud was not considered to be a priority of law enforcement. However, the Executive Director said that insurers now have increased their anti-fraud efforts because they recognize that health care fraud is widespread and because law enforcement (federal and state) has taken a significant interest in investigating and prosecuting such fraud. Accordingly, NHCAA still supports federal immunity legislation.

Health Insurance Association of America

In 1993, the Health Insurance Association of America conducted a survey to determine the extent to which its member companies engaged in health care anti-fraud activities. The survey asked for the number and types of cases the companies investigated each year from 1990 through 1992. During each year of the survey period, member companies referred only 9 to 11 percent of their cases to law enforcement agencies.[11] In 1992, for example, the companies investigated a total of 26,755 health insurance fraud cases but referred only 2,645 cases (or about 10 percent) to law enforcement agencies. According to an Association official, this relatively

[9]NHCAA Board of Governors, "Maximizing Private-Public Cooperation in Fighting Health Care Fraud—Principles and Policy Options to Strengthen the Private Sector's Anti-Fraud Capability" (Washington, D.C.: August 1993).

[10]Health Care Fraud: Hearings Before the Subcommittee on Crime and Criminal Justice of the House Committee on the Judiciary, 103d Cong., 1st Sess. (February 4 and May 27, 1993).

[11]Eighty-six companies responded to the survey. Of these, 79 are commercial insurers representing 65 percent of the commercial market; the other 7 are Blue Cross/Blue Shield plans representing 14 percent of the Blue Cross/Blue Shield market.

low referral percentage is due, in part, to insurers' concerns about potential civil liability.[12] This official further commented that the survey results indicate that federal legislation (preempting a "hodgepodge" of inadequate state statutes) is needed to provide immunity for insurers and others who provide fraud-related information to law enforcement authorities.

Medical Associations

An attorney in the American Medical Association's Health Law Division told us that although the Association has not formally commented on the immunity provisions contained in the various health care anti-fraud and abuse bills introduced in Congress, the Association generally supports immunity for reporting suspected health care fraud because it recognizes the benefits to anti-fraud enforcement efforts. Therefore, the Association supports immunity for insurers that report suspected fraud to law enforcement entities, as well as for insurers sharing fraud-related information with each other. The attorney said, however, that since medical information is sensitive and private in nature, any legislation that grants immunity for insurer-to-insurer information sharing should include controls to ensure that the information is not used inappropriately. He explained that the legislation could include, for example, a requirement that shared information must have a certain level of specificity or credibility—such as confirmed (rather than unsubstantiated) fraud allegations.

Representatives from several other medical associations, including the American Hospital Association, the American Health Care Association, and the National Association for Home Care, also indicated that their groups supported immunity protection. These representatives told us that their respective associations had not formally commented on the immunity provisions in any of the health care anti-fraud bills introduced in Congress, but they generally support the concept of immunity to protect individuals who report suspected fraud, as long as the immunity is qualified. That is, an immunity provision should include qualifications, such as absence of bad faith or malice, so that an individual who is actually harmed by a report of suspected fraud has a basis for filing a lawsuit.

[12]Reasons other than concerns about civil liability may have also been contributors to the relatively low referral percentage. From our field work, for example, we learned that insurance companies may focus on internally recovering overpayments versus pursuing fraud prosecution.

Our Interviews With Fraud Investigators and Prosecutors

As noted in chapter 1, to better understand whether broad federal immunity is needed, we interviewed individuals responsible for investigating and prosecuting health care fraud cases—officials at 12 federal and 6 state investigative and prosecutive offices and investigators and general counsel at 13 insurance companies (see app. I).

Views of Federal Government Officials

At 8 of the 12 federal investigative and prosecutive offices we visited, officials told us they believed a federal immunity law is needed to enhance anti-fraud enforcement efforts. The officials generally commented that a federal law may increase insurers' willingness to report fraud. In one location we visited, an FBI supervisory agent told us that none of his office's active health care fraud investigations were initiated on the basis of reports from private insurers. The supervisory agent said that on the basis of informal discussions between insurers and FBI agents, insurers indicated they considered reporting health care fraud to his office but have not due, in part, to concerns about possible exposure to civil liability. The supervisory agent also commented that federal immunity legislation may encourage insurers to report suspected health care fraud. As support for this opinion, he cited his experience in investigating bank fraud cases and explained that leads or referrals from banks increased after federal immunity legislation was strengthened.[13] Federal officials at several of the field offices we visited also said that a federal law would be beneficial because it would provide a standard level of protection in all states. A U.S. Postal Inspection Service investigator told us that a federal immunity law would make it easier to investigate multistate fraud schemes because there would be no concerns about which state immunity statutes applied in specific cases.

Assistant U.S. Attorneys at one office we visited told us that the effects of a federal law would be difficult to predict. These attorneys also noted, however, that their district does not receive many health care fraud case referrals from private insurers, partially due to the insurers' concerns about being sued civilly for sharing health care fraud-related information with federal prosecutors. They further commented that since most fraud schemes affect both private and public health care plans, the government would benefit from increased private insurer fraud reports because more public program fraud could be identified.

Federal officials at four field offices told us a federal immunity law would not enhance anti-fraud enforcement efforts in their respective jurisdictions

[13]The Annunzio-Wylie Anti-Money Laundering Act of 1992 (Title XV of P.L. 102-550) granted broad immunity—from civil liability under any federal or state law or regulation—to financial institutions and their employees for reporting suspicious bank transactions.

because a high level of information sharing was already occurring. They added, however, that other jurisdictions might benefit from a federal law, and they cited increased information sharing as a possible benefit. In one of the states we visited, an FBI supervisory agent told us that the need for a federal immunity law possibly was being overstated by insurance company executives. The supervisory agent noted that at the field level, fraud-related information was being reported by insurers' special investigative units to FBI agents—either informally on the basis of established working relationships or formally in response to government-issued subpoenas.

Regarding the immunity provision in S. 1088, federal officials at four of the field offices we visited told us that the scope of the provision should be expanded beyond HHS and DOJ. The officials commented that immunity should be provided for reporting to other federal entities with health care fraud enforcement responsibilities, such as the U.S. Postal Inspection Service and the Internal Revenue Service, as well as with state law enforcement authorities or state insurance departments.

Also, federal officials at four of the field offices said that S. 1088 should be expanded to provide immunity for insurers sharing fraud-related information with other insurers. The officials said this type of information sharing would be beneficial because insurers would be able to work together and identify the extent to which a fraud scheme is affecting more than one insurance company. One FBI supervisory agent we spoke with commented that the FBI would benefit from insurers sharing information with each other because his office would receive from the insurers more fully developed cases that are more likely to be accepted. Further, an Assistant U.S. Attorney told us that fraud perpetrators would be more reluctant to routinely defraud multiple insurers if they knew insurers routinely shared fraud-related information. Several of the officials also told us, however, that a possible disadvantage to allowing insurer-to-insurer disclosures is the potential for insurers to use the information for other than legitimate anti-fraud purposes. An insurer might, for example, disallow a health care provider from providing services under its health plan because of reports of suspected fraud by another insurer, even though the allegations have not been substantiated.

Views of State Government Officials

The responses to our survey of the 50 state insurance commissioners (see app. III) indicated broad support for both state and federal immunity laws. For those 38 states that provided immunity at the time of the survey, 35 responded to our question about the positive effects from their respective

states' immunity laws.[14] Twenty-four of the 35 respondents believed their states' laws had positive effects on anti-fraud enforcement efforts. Almost all of these respondents (21) indicated the state immunity law increased reporting of suspected fraud. Two-thirds (16) indicated the immunity law increased information sharing, and over half (14) answered that the number of fraud cases investigated increased. Of the 35 respondents answering our question about the negative effects from their states' immunity laws,[15] 32 indicated there were no negative effects stemming from such legislation. The other respondents cited excessive sharing of questionable intelligence and increased workloads as possible negative effects.

Our survey also asked for opinions about the effectiveness of a federal immunity law in facilitating the sharing of fraud-related information between (1) private health insurers and federal/state law enforcement authorities, (2) private health insurers and federal/state regulatory authorities, and (3) two or more private health insurers.[16] Of the respondents who answered these questions, 33 (of 39) indicated that a federal law would be very or somewhat effective in facilitating fraud-related information sharing between private health insurers and federal/state law enforcement authorities, and 32 (of 38) answered that it would be very or somewhat effective in facilitating information sharing between private health insurers and federal/state regulatory authorities. Twenty-seven (of 36) respondents answered that a federal law would be very or somewhat effective in facilitating fraud-related information sharing between two or more private health insurers.

At three of the six state investigative and prosecutive offices we visited, officials told us they believe a federal immunity law is needed to enhance anti-fraud enforcement efforts. The officials cited several potential positive effects of such a law, including increased information sharing among insurers and law enforcement agencies. Also, the officials said that a federal law would provide a minimum level of immunity protection to private insurers located or otherwise doing business in states without immunity statutes. An official from one state fraud bureau told us that a federal law might encourage insurers to become more actively involved in identifying and reporting fraud at its earliest stages, thereby improving the likelihood of effective case development.

[14]See appendix III, question number 13.

[15]See appendix III, question number 14.

[16]See appendix III, question number 17.

On the other hand, state officials at the offices that did not see a need for a federal immunity law cited various reasons for their viewpoints, such as:

- A federal law is not needed because many health care fraud cases are handled at the state level.
- Regulation of the insurance industry historically has been a state responsibility, and a federal law would be seen as encroaching on that responsibility.
- A federal law would not have much effect because insurers have business-related reasons for not reporting fraud-related information.

Regarding the latter opinion, a state fraud bureau official told us that insurers' willingness to report suspected fraud generally depended more upon corporate policy than upon the existence or scope of immunity statutes. This official noted that some companies aggressively pursue fraud and seek prosecutions, while other companies prefer to settle matters internally.

Regarding the federal immunity provision in S. 1088, state officials at five offices told us that the proposal should be more comprehensive. They generally said that the bill overlooks the important role the states play in health care fraud detection and prosecution and should be expanded to provide immunity for reporting information to nonfederal government entities. One state Department of Insurance official told us that the bill may result in insurers sharing health care fraud-related information with only the federal government. He believes this would reduce information sharing between private insurers and the states. Also, because the federal government would not have the resources to investigate all case referrals, many of the health care fraud cases that normally could be addressed at the state level would go unaddressed at the federal level.

State officials at two offices told us that a federal immunity law should provide immunity for insurer-to-insurer sharing of fraud-related information. As a supporting example for this opinion, one official said that passage of a state statute allowing automobile insurance companies' special investigative units to exchange information about suspected fraudulent claims helped to decrease automobile insurance fraud in that state. Further, this official commented that since passage of the state statute, automobile insurance companies' special investigative units have been able to coordinate and report to law enforcement agencies more fully developed cases that are more likely to be accepted for prosecution. As with the federal investigators and prosecutors, however, a few of the state

officials also told us that a possible disadvantage of allowing insurer-to-insurer disclosures is the potential for insurers to use the information for other than legitimate anti-fraud purposes.

Views of Private Insurance Company Officials

At 12 of the 13 insurance companies we visited, representatives told us a federal immunity law would help anti-fraud enforcement efforts. They generally said that a federal law would be beneficial because it would provide immunity protection uniformly applicable in every state. The Director of Investigations at one insurance company told us that fraud schemes tend to cut across state lines, typically affect more that one payer, and usually involve both public and private insurance programs. He added that a federal law would provide consistent protection during multistate or national fraud investigations, something that is not provided under the various state laws. Further, representatives of another insurance company said that a federal law would likely solve the problem of deciding which state's immunity laws take precedence in multistate investigations.

Representatives of several insurance companies also told us a federal law might result in more health care fraud case referrals to law enforcement agencies. They generally said the weight a federal law carries may encourage some insurers, who might not otherwise come forward under a state law, to report health care fraud cases to law enforcement agencies. Representatives from one national insurance company told us that they are aware of instances of fraud being committed against their company, but due to such factors as the lack of state immunity laws or poorly written state immunity laws, the company may internally address this fraud rather than refer it to law enforcement agencies. An attorney from another insurance company told us that a federal law could even help reduce the costs of defending against reactionary civil lawsuits because such legislation may provide a basis for summary judgments.

One insurance company investigator told us a federal law is not needed because insurance regulation is a state responsibility, and states are addressing this issue by passing legislation to provide immunity. He further commented that some insurers, as a business decision, will be reluctant to get involved in reporting fraud no matter what immunity protection, federal or state, is provided. The investigator added, however, that a federal law would still be beneficial to national insurers because it would provide some consistency in immunity protection, which is not now the situation under the various state laws.

Regarding the federal immunity provision in S. 1088, representatives of seven insurance companies told us that the immunity provision should be expanded to cover reporting to entities other than just HHS and DOJ. They said that immunity should be provided for sharing fraud-related information with other federal, as well as state, government entities that investigate or prosecute health care fraud. One company's investigator said that S. 1088 might be problematic because the FBI does not have enough resources to address the additional referrals the agency would likely receive. A Director of Investigations at another insurance company told us the bill overlooks the large number of cases that are prosecuted at the state level of government because they do not involve large enough dollar losses to be of interest to the federal government.

Representatives of nine insurance companies told us a federal law should provide immunity for insurer-to-insurer sharing of fraud-related information. These individuals generally said that allowing insurer-to-insurer information sharing would enable the companies to develop more significant cases—that is, cases involving larger dollar amounts and/or fraud schemes of wider scope—for referral to law enforcement agencies. Representatives from one insurance company told us that the quality of evidence will improve, resulting in more criminal prosecutions for health care fraud offenses. These representatives explained that by working cooperatively together, insurers will be able to show that multiple insurers were defrauded under the same scheme, and this will make it easier to prove the criminal element of intent (i.e., the suspects knowingly defrauded the insurers). To demonstrate the drawbacks of insurance companies not sharing fraud-related information with each other, the representatives noted the California "rolling labs" case.[17] They told us that the rolling labs fraud scheme was able to continue for years without being detected and reported to law enforcement agencies because the insurers were reluctant to work together to identify and determine the full scope of the fraud scheme. The representatives further commented that the rolling labs case is what prompted the state of California to enact strong immunity laws.[18]

Similar to the concerns voiced by some of the federal and state investigators and prosecutors we interviewed, a few of the insurance

[17]During a 10-year period beginning in 1981, a company operating mobile medical laboratories ("rolling labs") was able to perpetrate a billion-dollar fraudulent billing scheme that affected 1,400 insurance plans.

[18]As shown in appendix II, California law provides immunity for insurer-to-insurer information disclosures.

company representatives told us that a possible disadvantage to allowing insurer-to-insurer disclosures is the potential for the information to be used for purposes other than fraud detection and prevention. One insurance company investigator said that to ensure against unfair or conspiratorial practices by insurers, a federal law allowing insurer-to-insurer sharing of fraud-related information should include parameters covering what information can be shared (e.g., only information that clearly shows fraud occurred) and specifically who in the insurance companies can have access to the information (e.g., only special investigative units).

Conclusions

Immunity laws are designed to encourage insurers and other individuals to report suspected fraud by providing them protection against subsequent civil lawsuits related to such information sharing. Currently, there is no federal immunity protection for persons who report fraud-related information to law enforcement agencies. Statutory protection is provided for reports made about Medicare and Medicaid health care services to peer review organizations. However, insurers—the primary processors of health care claims—are not provided federal immunity protection for sharing fraud-related information concerning other public and private health plans. While most states have enacted immunity laws that provide some immunity protection to insurers, these laws vary from state to state.

The law enforcement, regulatory, and industry officials we queried expressed widespread support for the concept of a broad federal immunity law that includes adequate safeguards against bad faith allegations. As benefits of a federal law, these officials cited increased information sharing by insurers and uniformity of coverage in every state. Many of the officials, however, told us that to be most useful, a federal immunity law should provide broader protection than the immunity proposed under pending congressional bill S. 1088. The officials favored immunity for insurers, not just for sharing fraud-related information with DOJ and HHS, but for sharing such information with any federal or state entity with health care fraud enforcement responsibilities. They also favored expanding the immunity provision to protect insurers for sharing information with other insurers. One potential drawback to the latter approach is the possibility that insurers would inappropriately use information obtained from other insurers. While this is a potential risk of allowing insurer-to-insurer information sharing, the risks may be decreased through precise statutory language that specifies the reasons

and procedures by which insurers may share fraud-related information with other insurers.

Comments and Our Evaluation

DOJ provided technical and clarifying comments, which we incorporated where appropriate.

In its written comments on the draft report, NHCAA wholeheartedly endorsed the need for a federal immunity statute and commented that such a statute could play a significant role in expanding the private sector's ability to initiate investigations and cooperate with law enforcement. To be fully effective, NHCAA suggested that the federal statute should

- provide immunity protection with respect to all health care anti-fraud investigative activities;
- extend to all law enforcement officers, not just those connected to the administration of the health care system;
- apply to exchanges of information between private sector fraud investigators, i.e., information sharing between or among insurers;
- require that any allegation of sharing false information be "pled with particularity," a term of art under the Federal Rules of Civil Procedures; and
- allow the recovery of attorney fees to a payer that is sued and subsequently found to be entitled to immunity.

In its written comments on the draft report, the American Medical Association generally supported immunity for reporting fraudulent practices because it assists law enforcement efforts to bring perpetrators to justice. The Association added that any legislation granting immunity for insurers and any other entities to share information regarding suspected fraudulent behavior should include the following safeguards to ensure that such information is not used inappropriately:

- The shared information must be related to specific conduct, and the conduct must be outside the realm of legitimate disagreements on what care is medically necessary.
- There must be some substantiation of the information, so that its credibility is not in question.
- There must be an opportunity for one who is harmed by "bad faith" sharing of information to seek legal recourse.

Centralized Health Care Fraud Database May Be Beneficial but Some Questions Remain

Currently, there is no centralized national database in law enforcement to track patterns of criminal activity in the health care system. As a result, investigators and prosecutors use a variety of federal, state, and private industry databases to investigate health care fraud. To enhance access to health care fraud-related information and to help coordinate enforcement efforts, the proposed Health Care Fraud and Abuse Prevention Act of 1995 (S. 1088) calls for establishing a national, centralized database of health care fraud information. The proposed database would contain information about final adverse actions—such as license revocations, administrative sanctions, civil judgments, and criminal convictions—involving health care system participants. Such a database could be widely accessible, and it would assist investigators in developing background profiles on providers and other individuals under investigation.

Many law enforcement and industry officials told us they support the establishment of a database of final adverse actions, but it is not essential to their enforcement efforts. Although this type of database could be widely accessible to federal, state, and private investigators, the benefits of such a database may not justify the largely unknown costs involved to operate it. These officials suggested two alternative databases—one including ongoing investigative information and another including suspected fraud referrals—that might provide more investigative benefits than a database of final adverse actions. But, in addition to unknown costs, such databases would be much riskier in terms of the need to protect against unauthorized disclosure and use of the information.

Databases and Other Information Resources Useful to Health Care Fraud Investigators

Currently, there is no centralized national database in law enforcement to track patterns of criminal activity in the health care system. In an effort to obtain information on potential suspects and fraudulent schemes, health care fraud investigators can query various federal, state, and industry databases and other information resources (see app. IV). Data obtained from these systems can provide investigators with information needed to develop a comprehensive background profile on health care fraud suspects. Such data can also be useful to prosecutors in their efforts to obtain harsher sentences for recidivists. Although the databases and other information resources identified in appendix IV can be useful to investigators, each has certain limitations or disadvantages, as discussed below.

Federal Resources

Although the FBI's National Crime Information Center is the nation's most extensive criminal justice information system, the Center's criminal history records are accessible only by authorized federal, state, and local criminal justice agencies. Private sector entities, such as insurance company investigative units, do not have direct access to these records. In addition, the records are not easily identifiable as relating to health care fraud. For example, because there is no federal health care fraud statute, federal criminal convictions for health care fraud could have been obtained under any of several general statutes involving mail fraud, false statements, or conspiracy. Finally, the Center does not have records of noncriminal actions—such as federal and state civil judgments—taken against health care providers.

The HHS sanctions information, although nationwide in scope, covers only program exclusions taken against health care providers and practitioners for two public programs, Medicare and Medicaid. Although HHS recently began making its sanctions information more widely available, HHS does not identify individuals and entities sanctioned by Social Security or tax identification number. According to one insurance company official we interviewed, these identifiers are needed in order to make the sanctions data more useful for investigative purposes. This investigator explained that his company first had to crossmatch the names from the HHS sanctions report against another computer software program that contained names and Social Security/tax identification numbers; once that was done, the data were then downloaded into the company's computer system for future use.

Another federally sponsored information resource, the National Practitioner Data Bank, contains information on some, but not all, adverse actions taken against licensed health care practitioners. For example, it does not contain information about criminal convictions or civil judgments involving health care fraud. In addition, neither law enforcement agencies nor insurance company investigative units currently have access to the information in the Data Bank.

While concentrating on investigations that are national or international in scope, the Financial Crimes Enforcement Network (FinCEN) uses the majority of its resources to assist law enforcement agencies in their investigations of financial aspects of the illegal narcotics trade. However, for other financial crimes (such as health care fraud) that may involve money laundering, investigators can use FinCEN for intelligence and

analytical support to help identify and trace assets for seizure and forfeiture purposes.

State Resources

The National Association of Insurance Commissioners databases maintain nationwide information on regulatory and disciplinary actions taken against insurance agents and companies. This information is similar to that in the National Practitioner Data Bank, but it focuses on insurers and their agents rather than on health care providers. The Association's information on regulatory and disciplinary actions is publicly accessible and focuses on all lines of insurance, including health. However, the information on adverse actions taken—for example, an insurance agent's license revocation—is not necessarily related to fraudulent activity.

Industry Resources

NHCAA's Provider Indexing Network System is available to member companies and participating law enforcement agencies, all of whom agree to abide by established procedures governing when and what type of information can be submitted, how data are to be updated, and what limited uses can be made of System data. On-line access to this database is limited to NHCAA member insurance companies and law enforcement members, such as HHS' Office of Inspector General and the U.S. Postal Inspection Service. Nonmember law enforcement agencies can query the database through written request to NHCAA.

Another limitation is that the System is not comprehensive, containing only about 1,984 entries as of March 1996. Many private insurers are not members of the Association. Further, even NHCAA members are not required to report fraud-related information to the Association's database. Generally, in and of itself, information in the database is not "evidence" of any kind of fraudulent activity; rather, the information represents merely a means of focusing—in each member organization's independent discretion—limited investigative resources.

Every private payer that participates in the System agrees to indemnify the other participants if liability results from misuse of database information. However, one NHCAA member company's officials told us that their company does not provide information to the database due to concerns about how other members might access and use the information.

Another industry information resource potentially useful to health care investigators is the National Insurance Crime Bureau. Although the Bureau

was established to coordinate the insurance industry's efforts to address fraudulent claims involving automobile and other property/casualty insurance, its information systems may contain information relevant to certain health care fraud cases. For example, schemes involving staged automobile accidents or fraudulent workers compensation claims may entail fraudulent medical claims, sometimes involving corrupt health care providers in the scheme as well. Thus, while not all-inclusive, the Bureau's information systems may contain some information about individuals involved in suspected health care fraud.

Recent Proposals Would Create a National Database of Health Care Fraud-Related Information

To address the issue of access to health care fraud-related information, recent proposals (see table 3.1) have supported the establishment of a centralized repository for health care fraud information.

Table 3.1: Recent Proposals to Create a National Database of Health Care Fraud-Related Information

	Recent health care fraud database proposals		
Proposal elements and status	**Bush Administration's Health Care Fraud Task Force (1993)[a]**	**H.R.3600: Health Security Act (1993)**	**S.1088: Health Care Fraud and Abuse Prevention Act (1995)**
Type of information to be included in database	Two databases: (1) final adverse actions and (2)active fraud investigations	Data necessary to determine compliance with health care fraud statutes[b]	Final adverse actions
Management of database	Final adverse actions: HHS Active fraud investigations: HHS or DOJ	National Health Board	HHS
Access to information in the database	Final adverse actions: Law enforcement agencies, insurers, and private individuals Active fraud investigations: Law enforcement and state licensing agencies, and insurers with accredited anti-fraud units	Not specified	Federal and state government agencies and health plans
Status of proposal	Not implemented	Not enacted	Incorporated into 1996 Senate Budget Reconciliation Act (pending as of December 1995)

[a]The Bush Task Force recommended two national databases with different parameters.

[b]As discussed in the text, this database would contain more than simply information about fraud.

Source: GAO analysis of health care fraud proposals.

In January 1993, a Bush administration task force on health care fraud and abuse recommended the establishment of two national databases—one for the reporting of final adverse actions and one for active fraud investigations.[1] Access to the final adverse actions database would include not only law enforcement agencies, but also insurers and private individuals; access to the active investigations database would be restricted to law enforcement agencies, state licensing agencies, and insurance company investigative units. Regarding the final adverse actions database, the task force suggested—as an alternative to establishing a new database—expanding the National Practitioner Data Bank to require reporting of all final adverse actions involving practitioners and to include similar information about health care entities other than practitioners. Regarding the active investigations database, the task force also

[1]Final adverse actions include criminal convictions, civil money penalties, exclusions from federal health programs, and final actions taken by private insurers related to fraud and abuse. Active investigations include any ongoing investigations of potentially fraudulent activities.

recommended that participants be provided with good faith immunity for reporting to and obtaining information from the database as an incentive to encourage participation. Neither of the task force's database recommendations was implemented; however, the concept of a centralized health care fraud database has continued to be included in subsequent proposed federal legislation.

In November 1993, for example, the Clinton administration's proposed Health Security Act (H.R. 3600) advocated establishing a health information database containing, among other things, "information necessary to determine compliance with fraud statutes." However, because this act would have substantially reformed the nation's entire health care system, the proposed database was expected to contain much more than just information related to fraud. For instance, the database would have included information about clinical encounters and other health services provided, administrative and financial transactions of participants, utilization management by health plans or providers, and other nonenforcement-related activities and services. By late summer 1994, the original Clinton health reform bill had been essentially dropped by both the House and the Senate. Although proposals to establish a centralized health care fraud database appeared in several other health reform bills introduced during 1993 and 1994, none of these proposals were enacted.

In July 1995, Senator William Cohen introduced S. 1088, which includes a proposal to establish a centralized repository for the reporting of final adverse actions against health care providers, suppliers, or practitioners.[2] As defined in this bill, the term "final adverse action" includes (1) civil judgments against a health care provider in federal or state court related to the delivery of a health care item or service; (2) federal or state criminal convictions related to the delivery of a health care item or service; (3) actions by federal or state agencies responsible for the licensing and certification of health care providers, suppliers, and licensed health care practitioners; (4) exclusions from participation in federal or state health care programs; and (5) any other adjudicated actions or decisions that the HHS Secretary establishes by regulation. In October 1995, this legislative proposal was incorporated into the Senate's proposed 1996 Budget Reconciliation Act, which was still pending at the time of our review.

[2]This proposal was originally introduced by Senator Cohen in January 1995 as part of S. 245 and was later incorporated into S. 1088.

While advocating the establishment of a centralized health care fraud database, none of the proposals noted above clearly identified the database's expected operating parameters—such as how many data records would be maintained, how many information queries were expected, and how much the system might cost to develop and operate.[3] Current systems that might be useful in evaluating the recent health care fraud database proposals are the National Practitioner Data Bank, a system containing data on certain final adverse actions; and the Provider Indexing Network System, a system containing data on active investigations.

As a large, national repository containing certain information on adverse actions taken against health care practitioners, the National Practitioner Data Bank illustrates how a centralized health care fraud database might be expected to operate. As of December 1994, the Data Bank contained over 97,000 records. The Data Bank has received over 4.5 million inquiries since it became operational in 1990, with the number of annual inquiries increasing from about 800,000 in 1991 to just over 1.5 million in 1994. The original 5-year contract (awarded in December 1988) to develop and operate the Data Bank was expected to cost $15.8 million. According to HHS officials, this contract was subsequently extended through June 1995, and the estimated cost was expected to be $24 million. Total costs to operate the Data Bank—including contract and HHS administrative costs—averaged almost $5.8 million annually for the period 1991 through 1994. The next operating contract—for the so-called second generation Data Bank—is expected to be less costly, about $12 million over 6 years. By law, Data Bank inquiry processing costs can be recovered through user fees, which currently range from $4.00 to $10.00 per inquiry.

Although much smaller in scope and concept than the National Practitioner Data Bank, the NHCAA's Provider Indexing Network System is a centralized repository of investigative information dealing specifically and solely with health care fraud. Because it is a personal computer-based system, the costs to develop and operate the system—about $30,000 to develop and about $35,000 (fiscal year 1995 costs) to operate—are much less than those incurred by the mainframe computer-based National

[3]For instance, according to Congressional Budget Office staff, there has been no formal cost estimate ("scoring") of S. 1088, which included a provision (Section 301) calling for establishment of a "Health Care Fraud and Abuse Data Collection Program." However, in response to our inquiry, the staff told us that—based upon information obtained from the Health Resources and Services Administration and from experience with the National Practitioner Data Bank—implementation of Section 301 would cost $2 million in unrecovered start-up costs in the first year. The staff explained that this estimate is based upon the assumption that Section 301 implementation would be tied into the existing National Practitioner Data Bank, rather than establishing a new and separate centralized system.

Practitioner Data Bank. However, the relatively low costs are also reflected in the size of the database, which included only 1,984 entries as of March 1996. Although the size of the Provider Indexing Network System might limit its usefulness as a national information resource, it does demonstrate a less expensive alternative approach to health care fraud information sharing.

Law Enforcement and Industry Have Mixed Views on the Benefits of a Centralized Health Care Fraud Database

As noted in chapter 1, to better understand the advantages and disadvantages of a centralized health care fraud database, in 4 states we interviewed individuals responsible for investigating and prosecuting health care fraud cases at 12 offices of federal agencies, 6 offices of state agencies, and 8 insurance companies; and in 2 other states, we interviewed investigators and general counsel at 5 national insurance companies (see app. I).

Limiting a Centralized Database to Only Final Adverse Actions

As shown in table 3.1, recent legislative proposals have supported the establishment of a centralized health care fraud database of final adverse actions. The 1993 Bush Administration Health Care Fraud Task Force and the proposed 1995 Health Care Fraud and Abuse Prevention Act both specifically supported the establishment of a centralized repository for the reporting of final adverse actions against practitioners, providers, and other health care entities.[4] In general, final adverse actions have been adjudicated in some federal or state public forum (for example, before courts or health care licensing and certification agencies) and are considered to be generally available to the public.

Views of Federal Government Officials

Officials at 5 of the 12 federal investigative and prosecutive offices we visited told us they believe a centralized database of final adverse actions would be useful to health care fraud enforcement efforts. At three of these offices, officials told us that the database would make it easier for health care fraud investigators to do the background work necessary to establish a suspect's past history of fraudulent activity. A U.S. Postal Inspection Service investigator noted that even though this information is already publicly available, having it all located in one repository would make the investigative process more timely. Officials at four of these offices indicated that knowing whether a suspect has been found to have committed past fraudulent acts would make it easier for prosecutors to

[4]As noted previously, although the Clinton administration proposal advocated establishment of a national health information database, it did not specify the inclusion of final adverse actions in the database.

demonstrate the individual's intent to defraud. One Assistant U.S. Attorney noted that having easy access to past histories of fraudulent activity not only helps to prove an individual's intent to defraud, but also can be used to demonstrate prior relevant conduct that would support an increased criminal sentence.

At 6 of the 12 offices we visited, officials noted that although establishment of such a database is not critical to enforcement efforts, there could still be some benefits. These officials generally noted that the information was already publicly available from other sources and other information was more useful.

Officials at one office we visited told us they did not believe it necessary to establish a final adverse actions database. According to an Assistant U.S. Attorney, the information that would be in the database is already publicly available from other sources and, given the current government budget environment, he questioned the feasibility of funding a database that would provide only marginal enforcement utility.

Most of the officials we spoke with expressed some concerns about the establishment of a final adverse actions database. Most notably, at eight offices, officials indicated that the potential would exist for the information to be misused—for example, by insurance companies to deny a provider's insurance claims or by the government in targeting persons for investigation. One FBI supervisory agent told us that to ensure the security of the database and prevent misuse, access should be restricted to law enforcement agencies only. At six offices, officials stated that providers and the public would likely object to the establishment of such a database as an unwarranted intrusion by the federal government into the privacy of citizens' lives. One Assistant U.S. Attorney noted that having the federal government operate the database might also result in the database becoming too bureaucratic and entangled with rules and regulations about access, thereby making the database less efficient to operate.

Views of State Government Officials

The responses to our survey of the 50 state insurance commissioners indicated broad support for a centralized health care fraud database. Of the 29 respondents who said their offices investigated health care fraud during 1994, 26 believed a centralized health care fraud database would facilitate enforcement efforts.[5] Twenty-three of the respondents indicated that a database would expedite the enforcement process, with about half indicating that it would either strengthen prosecution efforts or lead to

[5]See appendix III, question number 21.

harsher penalties. The respondents were split on who should operate the database, with about 10 favoring the federal government, 8 favoring state government, and 7 favoring the private sector.[6] Twenty-seven of the respondents indicated that final adverse actions should be included in the database.[7] Eighteen of the respondents also believed there might be some negative effects of a centralized health care fraud database, most notably the lack of security and confidentiality of the information (12) and the possibility that the database would contain inaccurate information (13).[8]

At three of the six state investigative and prosecutive offices we visited, officials we interviewed told us they believe a centralized health care fraud database of final adverse actions would be useful in facilitating health care fraud enforcement efforts. At the other three offices, officials noted that such a database is not essential but could be another tool to assist health care fraud investigators. However, all officials saw certain advantages to a centralized database. The state officials noted, for example, that a centralized database would (1) provide investigators with easy access to information about individuals being investigated, thus making routine background investigative work more efficient; and (2) help investigators to better identify fraudulent schemes and potential suspects. One state fraud bureau official told us that because of the mobility of fraud perpetrators, a national database would help investigators to identify individuals within their jurisdictions who have been previously involved in fraudulent schemes in other locations.

At the five offices that identified possible negative effects of a final adverse actions database, officials said they were concerned that the information might be misused. One Insurance Department official stated that insurers might use the information, independently or in concert with other insurers, to unfairly restrict the ability of certain providers to participate in their health plans.

Views of Private Insurance Company Officials

At 9 of the 13 insurance companies we visited, representatives told us a centralized health care fraud database of final adverse actions would facilitate health care fraud enforcement efforts. At three of the companies, representatives thought the database might be beneficial, but they did not consider it an essential resource.[9]

[6]See appendix III, question number 23.

[7]See appendix III, question number 24.

[8]See appendix III, question number 22.

[9]One of the insurance companies did not comment on the database issue.

Most of the officials told us that a centralized repository of final adverse actions would make the investigative process more efficient by providing a single location for background information about health care providers who previously have been involved in fraudulent activity. One insurance company investigator noted that such a database could help insurers to easily identify providers with a previous record of fraud, which would allow insurers to more closely monitor future claims submitted by these providers. Another investigator mentioned that a centralized database would help insurers to better screen providers who have applied to join their health care network. The officials who believed a final adverse actions database was not essential generally said that the information would be useful for confirming suspicions or getting cases accepted for prosecution, but not for identifying and initiating investigations.

The most commonly voiced concern about establishing a final adverse actions database was potential misuse of the information. Officials at five insurance companies mentioned this as a potential problem. One insurance company official stated that creation of such a database might, from the providers' perspective, lead to the inappropriate identification and targeting of innocent individuals by investigators. One other official noted the possibility that inaccurate information could be included in the database and could have adverse consequences if inadvertently disclosed.

Including Ongoing Case Information in a Centralized Database

Only one of the recent database proposals—the 1993 Bush administration's proposal—would include active investigative information as part of a centralized health care fraud database. As described in the recommendations of the task force, this database would have been accessible to law enforcement entities, state licensing agencies, and accredited insurer special investigative units. The task force specifically defined active investigations as any ongoing investigation of potentially fraudulent activity. Ongoing investigative information is naturally more sensitive than information about final adverse actions, since at this stage of an investigation there has not yet been a public adjudication of the matter.

Views of Federal Government Officials

At 6 of the 12 investigative and prosecutive agencies we visited, officials told us a database of ongoing, or active, investigative information would be useful to health care fraud enforcement efforts. Officials at two of the six offices noted that the database would provide a means to identify multiple agencies investigating the same subject, thus helping to eliminate investigative duplication and allowing investigators to combine efforts.

More often, however, the officials cited concerns about an ongoing investigative database. At five of the six offices, officials cited the sensitivity of the information as a significant concern that would result in restricted access to the database. In general, the officials noted that for security reasons, such a database would probably have to be restricted to law enforcement agencies only. For example, according to one Assistant U.S. Attorney, sensitive investigative information (unlike final adverse actions) is, by its nature, less certain, sometimes inaccurate, and may never end up being adjudicated in a public forum. This official added that if such information is inadvertently or deliberately disclosed, it could seriously damage an individual's life and livelihood.[10]

Equally significant, Assistant U.S. Attorneys at two offices we visited noted that where investigative information was gathered through the federal grand jury process, it would be illegal to disclose that information to anyone not designated by the court. Similarly, all of the FBI officials we spoke with noted that the FBI would be very reluctant to contribute active investigative information to the database, unless the FBI controlled use of and access to the database.[11]

Views of State Government Officials

The responses to our survey of the 50 state insurance commissioners indicated support for including ongoing investigative information in a centralized health care fraud database. Of the 29 respondents who said they investigated health care fraud during 1994, 22 believed a database of ongoing investigative information would facilitate enforcement efforts.[12] Similarly, at three of the six state investigative and prosecutive agencies we visited, officials told us a database of ongoing investigations would be useful to health care fraud enforcement efforts.

However, one state fraud bureau official pointed out that because of the sensitivity of the information and the need for security, access to the database probably would have to be restricted to law enforcement agencies only. In this official's opinion, if insurance company investigators

[10]In commenting on a draft of this report, DOJ officials said that concerns about the misuse of data should include concerns about the integrity of the data being compromised, unless strict limitations are imposed regarding who can input and update the data.

[11]Restricting an ongoing investigative database to law enforcement agencies, however, is no guarantee of security. In the past, we have reported on misuse and inappropriate disclosures of sensitive information from the FBI's National Crime Information Center (National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information (GAO/T-GGD-93-41, July 28, 1993), a data system in which access and use are restricted solely to authorized criminal justice agencies for criminal justice purposes.

[12]See appendix III, question number 24.

are cut off from this valuable source of intelligence, they will not be as effective in their own anti-fraud efforts.

Views of Private Industry Officials

At 4 of the 13 insurance companies we visited, officials we spoke with identified an ongoing investigations database as being useful to health care fraud enforcement efforts. According to one insurance company investigator, having access to a database of ongoing investigations would provide investigators a means to combine efforts across jurisdictions. This investigator further commented that in many instances, any one insurer may have incurred only minimal dollar losses due to the fraud committed; however, fraud schemes are often perpetrated simultaneously in multiple jurisdictions. He said that if an investigator can identify other ongoing investigations targeting the same individuals, these investigations may be combined into a larger investigation. This would potentially allow investigators to develop larger, more significant fraud cases that are more attractive to prosecutors.

One indication of the potential positive effect of sharing ongoing investigative information can be found in recent statistics developed by NHCAA with regard to its Provider Indexing Network System. As of April 1995, NHCAA reported that 7.2 percent of the known or suspected fraud perpetrators listed in its computerized database had been entered by more than one member organization. These duplicate listings illustrate a potential opportunity for investigators in different organizations to share investigative information and possibly combine their enforcement efforts.

With regard to potential drawbacks, one insurance company investigator told us that insurers might be unwilling to report ongoing investigative information to the database if they are not granted access to it. Another insurance company official stated that insurers would have to be provided immunity for reporting such information because of the potential liability if the information were disclosed.[13] Demonstrating the reality of this concern, one investigator noted that her company will not place ongoing investigative information in NHCAA's Provider Indexing Network System because the company could not be sure that another member insurer would not misuse the information, thus exposing the reporting company to potential civil liability.

[13]Such immunity would have been provided to insurers under the Bush administration's proposal to create a database of active fraud investigations (see ch. 2).

Establishing a Database of Suspected Fraud Referrals

Although not identified in any of the recent health care fraud database proposals, one alternative to the two database approaches noted above is a database of suspected fraud referrals. Most health care fraud cases begin as fraud referrals to investigative agencies. These referrals come from both formal sources (e.g., government agencies, insurers) and informal sources (e.g., fraud hotlines, beneficiaries). The investigative agencies review these referrals and, on the basis of relatively limited information, select the most promising leads for assignment to an investigator. Because suspected fraud referrals typically have not yet been thoroughly investigated, they involve information that is less certain than information about either ongoing investigations or final adverse actions. There is a federal precedent for the creation of a fraud referral database. Such a database has been established at the Financial Crimes Enforcement Network to obtain and track information about suspected financial institution fraud.

Officials at 8 of the 31 federal, state, and insurance company offices we visited suggested the creation of a health care fraud referral database as a useful tool to enhance health care fraud enforcement efforts. Many of the respondents to our survey of state insurance commissioners also supported creation of a fraud referral database. Specifically, 22 of the 29 survey respondents who indicated they investigated health care fraud during 1994 favored creation of a fraud referral database.[14] In addition, the FBI has recently suggested that Congress pass legislation to create a criminal referral system, whereby all health benefit programs would be required to report suspected fraud to a federal government database to be used to track patterns of criminal activity throughout the health care system.[15]

Regarding potential benefits, one FBI supervisory agent told us that a database of suspected fraud referrals would expedite the early stages of an investigation by possibly helping to determine the extent and amount of fraud involved. An insurance company investigator also noted that encouraging private insurers to report suspected fraud to a national database would allow government investigators to better identify fraudulent schemes involving multiple private insurers and—since these schemes tend to involve both private and public sector insurers simultaneously—would very likely also lead to the discovery of more public sector fraud. According to an Assistant U.S. Attorney, in order to be most useful, a suspected fraud referral database would have to include

[14]See appendix III, question number 24.

[15]FBI, Health Care Fraud: Medical Fraud and Legislative Remedies, December 1994.

(1) a requirement for all insurers to report suspected fraud, along with a grant of immunity for doing so; (2) a specified reporting format; and (3) a designated entity to centrally collect and maintain the information.

Concerns were raised, however, about the feasibility of establishing a fraud referral database. For example, unlike the banking and savings and loan industries, the insurance industry is subject principally to state, rather than federal, regulation.[16] One FBI supervisory agent noted that access to suspected fraud referrals was helpful in fighting bank fraud, and a database of health care fraud referrals could help investigators initiate health care fraud cases. The agent said that to encourage private insurers to actively refer suspected fraud, ideally federal law should require mandatory reporting of such fraud and provide immunity for doing so. However, the agent believes that because there is no federal regulatory entity governing private insurers, such a law may not be possible.

According to an insurance company official, absent such a reporting requirement, private insurers may not feel compelled to report suspected fraud to a national referral database, thus making it less comprehensive in scope and, therefore, less useful to investigators. Also, many states already require insurers to report suspected fraud to state agencies (see app. II). According to a U.S. Postal Service investigator, in those states with suspected fraud reporting requirements, an additional federal reporting requirement might be viewed by some private insurers as being unnecessary.

In addition, because of the sensitive nature of suspected fraud referral information, several officials noted that security for and access to a database of suspected fraud referrals would likely be a critical issue. According to one FBI supervisory agent, some of the information in a suspected referral database might be nothing more than unsupported allegations, and the release or misuse of such information might ruin an innocent doctor's reputation or career. Therefore, access to and use of the information in the database would have to be tightly controlled. And, as pointed out by one Assistant U.S. Attorney, access to information of this nature would likely have to be restricted to law enforcement agencies only, in order to best protect against misuse and inappropriate disclosures.

[16]The 1945 McCarran-Ferguson Act affirmed the states' primary responsibility for regulating the insurance industry, including responsibility for establishing and enforcing rules under which insurers operate.

Conclusions

Recent proposals to establish a centralized health care fraud database, if implemented, would provide investigators and prosecutors an additional tool to enhance anti-fraud enforcement efforts. Senate Bill 1088 would establish a health care fraud database of final adverse actions, accessible by law enforcement and regulatory agencies and insurers. Law enforcement and industry officials identified certain other types of information—ongoing investigative information and reports of suspected fraud—that might also be useful to include in a health care fraud database. However, although these types of information would be potentially beneficial, they would also pose increased risks of inappropriate disclosure and misuse.

Many law enforcement, regulatory, and industry officials we spoke with agreed that a database comprising final adverse actions may benefit investigators only marginally. Although they said this type of information would be useful in compiling general background information on suspects, they added that it is already publicly available from other sources. However, the officials noted that disclosure of such information would likely pose minimal risks of civil lawsuits for violation of individuals' privacy rights. Ongoing investigation information has a lesser degree of credibility and a higher degree of sensitivity than final adverse actions information. The officials said that this type of information can be used to help build prosecutable cases; however, such information has not yet been adjudicated and would therefore have to be protected against inappropriate disclosures.

A database of suspected fraud referrals also poses risks from inappropriate disclosures. In many instances, minimal investigative time has been spent to verify the validity of fraud referral information. However, according to the officials we spoke with, such information can be useful to investigators in identifying previously undiscovered fraud. In addition to the issues noted above, centralized databases also pose uncertainties about development and operating costs. These costs generally have not been addressed by any of the proposals discussed above.

Comments and Our Evaluation

In its written comments on the draft report, NHCAA commented that a centralized database, if properly created, would be a useful additional tool in fighting health care fraud. As an analogy, NHCAA referred to the Provider Indexing Network System and said that a database is most useful when it (a) includes information on active investigations, (b) has safeguards and

procedures that are carefully outlined, and (c) has modest costs. Further, NHCAA commented that a centralized database would be particularly helpful if there is disclosure of information by both law enforcement agencies and private payers on a regular basis. Finally, NHCAA made some technical and clarifying comments, which we incorporated where appropriate.

In its written comments on the draft report, the American Medical Association supported the sharing of information related to fraud and abuse but said that creating a national database may not be the best use of limited enforcement dollars. The Association commented that databases can be exceedingly expensive to establish and maintain, have great potential for problems with inappropriate use and disclosure of information, and also may not sufficiently protect the confidentiality of patient records.

Organizations Contacted by GAO

As listed in tables I.1 and I.2, we contacted 12 offices of federal agencies, 6 offices of state agencies, and 13 private insurance companies.

Table I.1: Federal and State Agencies and Private Insurers Contacted in Four States

	Agencies		
State	**Federal**	**State**	**Private insurers**
Florida	U.S. Attorney's Office, Middle District of Florida (Jacksonville)	Department of Insurance, Division of Insurance Fraud (Tallahassee)	Blue Cross/Blue Shield of Florida (Jacksonville)
	U.S. Attorney's Office, Northern District of Florida (Tallahassee)		Nationwide Insurance (Gainesville)
	Federal Bureau of Investigation (Jacksonville)		
Maryland	U.S. Attorney's Office, District of Maryland (Baltimore)	Insurance Administration (Baltimore)	Blue Cross/Blue Shield of Maryland (Owings Mills)
	Federal Bureau of Investigation (Baltimore)	Office of the Attorney General (Baltimore)	U.S. Fidelity and Guaranty Company (Baltimore)
	Postal Inspection Service (Baltimore)	Maryland Insurance Fraud Unit (Baltimore)	
Massachusetts	U.S. Attorney's Office, District of Massachusetts (Boston)	Insurance Fraud Bureau (Boston)	Allmerica Financial (Worcester)
	Federal Bureau of Investigation (Boston)		Massachusetts Mutual Life Insurance Company (Springfield)
	Postal Inspection Service (Boston)		
Texas	U.S. Attorney's Office, Southern District of Texas (Houston)	Department of Insurance, Insurance Fraud Unit (Austin)	Blue Cross/Blue Shield of Texas (Richardson)
	Federal Bureau of Investigation (Houston)		GEICO Insurance (Houston)
	Postal Inspection Service (Houston)		

Table I.2: National Insurance Companies Contacted in Connecticut and Illinois

State	Insurer
Connecticut	Aetna Health Plans (Middletown)
	ITT Hartford Insurance (Simsbury)
Illinois	CNA Insurance Companies (Chicago)
	Kemper National Insurance Companies (Long Grove)
	State Farm Insurance Companies (Bloomington)

Comparison of State Immunity Statutes

State	Requires reporting of fraud?[a]	Immunity provided?	Statute grants	
			State law enforcement authorities	Insurance commissioner
AK	Yes	Yes		X
AL	No	No		
AR	No	Yes	X	X
AZ	Yes	Yes		X
CA	Yes	Yes	X	X
CO	No	Yes		X
CT	No	Yes		X
DE	Yes	Yes	X	X
FL	Yes	Yes	X	X
GA	Yes	Yes	X	X
HI	No	No		
IA	No	Yes	X	X
ID	Yes	Yes		X
IL	No	Yes	X	X
IN	No	Yes	X	X
KS	No	Yes	X	X
KY	Yes	Yes	X	X
LA	Yes	Yes	X	X
MA	Yes	Yes		
MD	Yes	Yes	X	X
ME	No	Yes	X	X
MI	No	No		
MN	Yes	Yes	X	X
MO	Yes	Yes		X
MS	No	No		
MT	Yes	Yes		X
NC	Yes	Yes		X
ND	Yes	Yes	X	X
NE	No	Yes	X	X
NH	No	Yes	X	X
NJ	Yes	Yes		X
NM	No	Yes	X	X
NV	Yes	Yes	X	X
NY	Yes	Yes		X
OH	Yes	Yes	X	X

immunity for sharing fraud-related information with					For grant of immunity there must be absence of			
Federal law enforcement authorities	Federal regulatory agencies	National Association of Insurance Commissioners	Other insurers	Other[b]	Malice	Bad faith	Fraudulent intent	Other[c]
					X			
X		X	X			X	X	
					X			
			X		X		X	X
					X	X	X	
					X			X
X		X	X		X	X	X	
		X	X	X	X	X	X	X
X						X	X	
X	X	X			X	X	X	
X					X		X	
X					X			
X	X	X		X	X	X	X	
X		X	X		X	X	X	
X	X	X			X		X	X
X	X	X			X	X	X	
				X	X	X		
X						X		
X		X		X	X	X	X	
X						X		
					X			
						X	X	
					X			
X	X	X	X		X			
X		X			X	X	X	
X	X	X	X	X	X			
					X	X		
X	X	X			X	X	X	
X		X			X			
					X	X	X	
X	X	X	X	X	X	X	X	

(continued)

State	Requires reporting of fraud?[a]	Immunity provided?	Statute grants: State law enforcement authorities	Statute grants: Insurance commissioner
OK	No	No		
OR	No	No		
PA	Yes	Yes	X	X
RI	No	No		
SC	Yes	Yes	X	X
SD	No	Yes	X	X
TN	No	No		
TX	Yes	Yes	X	X
UT	No	Yes	X	X
VA	No	No		
VT	No	No		
WA	Yes	Yes	X	X
WI	No	Yes		X
WV	No	No		
WY	No	No		

immunity for sharing fraud-related information with					For grant of immunity there must be absence of			
Federal law enforcement authorities	Federal regulatory agencies	National Association of Insurance Commissioners	Other insurers	Other[b]	Malice	Bad faith	Fraudulent intent	Other[c]
X	X				X	X		
X					X			
X					X	X		
X	X	X			X	X	X	
X					X	X	X	
X					X			
					X			

Note: Survey responses about state immunity laws were not independently verified by GAO.

[a]Applicable state statutes generally apply to all types of insurance fraud and do not focus specifically or soley on health care fraud. The reporting requirements vary by who is required to report suspected fraud and to whom the report is made.

[b]Florida also grants immunity for sharing with the National Insurance Crime Bureau; Indiana also grants immunity for sharing with any organization established to detect and prevent fraudulent insurance acts; Massachusetts grants immunity only for sharing with the fraud bureau (which is not a state law enforcement entity); Maine also grants immunity for sharing with organizations established to detect and prevent fraudulent insurance acts; New Hampshire also grants immunity for sharing with any state or federal agency established to detect, prevent, or prosecute insurance fraud; and Ohio grants immunity for sharing with any person involved in the detection or prevention of fraudulent insurance acts.

[c]California also requires absence of willful intent (as defined in California Penal Code); Connecticut also requires absence of willful intent to injure any person; Florida also requires absence of reckless disregard for the rights of any insured; and Kentucky also requires absence of gross negligence.

Source: GAO survey of state insurance commissioners.

State Insurance Commissioners Health Care Fraud Survey

STATE INSURANCE COMMISSIONERS HEALTH CARE FRAUD SURVEY

United States General Accounting Office

State Insurance Commissioners Health Care Fraud Survey

INTRODUCTION

The U.S. General Accounting Office (GAO), an agency of Congress, is studying federal and state efforts to address health care fraud, including the extent to which private insurers share potential fraud-related information within the industry and with government investigators and prosecutors. As part of this study, GAO is surveying the extent to which states have enacted laws providing immunity to private health insurers who share fraud-related information for enforcement purposes. Also, GAO is seeking state officials' views about whether additional enforcement tools, such as a federal immunity provision and a central repository for health care fraud information, would help encourage further information sharing on health care fraud matters.

This survey should take about 30 minutes to complete. If you have any questions or need assistance in completing the survey, please call Philip Caramia (214-777-5637) or Warren Lundy (214-777-5607).

Please return the completed survey in the enclosed pre-addressed envelope within 10 days of receipt. In the event the envelope is misplaced, the return address is

U.S. General Accounting Office
Dallas Regional Office
Attn: Mr. Phil Caramia
1445 Ross Avenue, Suite 1500
Dallas, TX 75202

Thank you for your assistance.

1

I. SURVEY INFORMATION

INDIVIDUAL COMPLETING THIS SURVEY:

Name: _____

Title: _____

Organization/office: _____

Address: _____

_____

Phone: ( )_____ Fax: ( )_____

STATE INFORMATION:

Approximate size of office:

Number of full- and part-time investigators:

full-time_____ part-time_____

Total number of full- and part-time staff:

full-time_____ part-time_____

Number of private insurers writing business in state:_____

Number of private health insurers writing business in state:_____

DEFINITIONS:

Health care fraud - Health care fraud is defined as:
(1) schemes by practitioners, corporate health providers, or private individuals to defraud health insurers, or
(2) schemes by brokers, agents, or insurers to defraud beneficiaries or regulatory agencies, or
(3) payment of kickbacks to influence medical practices, or
(4) schemes involving illegal, unlicensed, or substandard provision of health care.

Reference year - Answers should refer to your office's activities during calendar year 1994. If your office normally follows another reference year for reporting or operational purposes (fiscal year, for example), please refer to that year in making your responses and indicate below the reference year used:

*** [From _____ 19___ to _____ 1994.] ***

II. STATE HEALTH CARE FRAUD ENFORCEMENT AND REGULATORY ENVIRONMENT

In January 1994, the U.S. Attorney General designated health care fraud as the Justice Department's number two enforcement priority (behind violent crime). To carry out this directive, the Attorney General designated a Special Counsel for Health Care Fraud to coordinate health care anti-fraud enforcement efforts between the Justice Department and other public and private sector organizations responsible for investigating and prosecuting health care fraud.

1. Does your state have a statute defining and prescribing penalties for insurance fraud?

   1 _12_ No --> *(**Skip to question 3**.)*

   2 _38_ Yes --> 1a. Please cite the applicable statute(s):

   _____

   _____

   _____

2. Which of the following types of health care fraud, if any, are applicable under your state's insurance fraud statute(s)? *(Mark all that apply.)*

   1 _33_ Fraud committed against health insurers
   2 _29_ Fraud committed by health insurers or agents
   3 _21_ Fraud involving illegal payments to medical practitioners
   4 _11_ Fraud involving illegal, substandard, or unlicensed medical care
   5 __8_ Other *(Please specify)* _____

   _____

   _____

   6 __2_ Does not apply to health care fraud

3. Does your state have a specialized insurance investigative unit or fraud bureau?

   1 _12_ No

   2 _36_ Yes --> 3a. What types of fraud does the unit investigate? *(Mark all that apply.)*

   1 _29_ Health care fraud *(as defined on page 2)*
   2 _25_ Workers compensation fraud
   3 _27_ Property/casualty fraud
   4 _22_ Other *(Please specify)* _____

   _____

   _____

4. During calendar year 1994, about what percent of your office's investigative caseload was made up of cases involving health care fraud? (*Mark one in each category.*)

1 __18__ 1-10%
2 __6__ 11-20%
3 __2__ 21-30%
4 __2__ 31-40%
5 __1__ 41-50%
6 __0__ Greater than 50%

7 __18__ No cases involving health care fraud were investigated in calendar year 1994.

5. Overall, during the past three calendar years (1992 through 1994), has the percentage of your office's investigative caseload involving health care fraud... *(Mark one.)*

1 __6__ increased greatly,
2 __11__ increased somewhat,
3 __20__ remained about the same,
4 __0__ decreased somewhat, or
5 __0__ decreased greatly?

6. In calendar year 1994, did your office refer any investigative cases involving health care fraud to...

a. city or county investigators?

1 __7__ Yes
2 __28__ No

b. city or county prosecutors?

1 __15__ Yes
2 __22__ No

c. the state attorney general?

1 __14__ Yes
2 __24__ No

d. federal investigators?

1 __17__ Yes
2 __22__ No

e. federal prosecutors?

1 __10__ Yes
2 __26__ No

4

7. In calendar year 1994, in which of the following health care fraud coordinating activities, if any, did your office participate? *(Mark all that apply.)*

1 11 State/Local health care fraud task force
2 11 Federal health care fraud task force
3 8 U.S. Attorney's Health Care Fraud Working Group
4 13 Interagency health care fraud training, conference, or meeting
5 13 Other health care fraud coordinating activities *(Please specify)*

_____

_____

_____

6 24 The office did not participate in any health care fraud coordinating activities

8. During calendar year 1995, does your office expect to increase its focus on health care fraud?

1 25 Yes --> 8a. If yes, why? *(Mark all that apply.)*

1 13 Health care fraud becoming a major problem
2 2 Increased legislative funding
3 6 Additional resources available
4 15 Other reason *(Please specify)*

_____

_____

_____

2 24 No --> 8b. If no, why not? *(Mark all that apply.)*

1 1 Health care fraud is not a major problem
2 2 Other types of fraud are higher priority
3 12 Lack of available staff
4 5 Lack of health care fraud expertise
5 15 Other reason *(Please specify)*

_____

_____

_____

5

III. IMMUNITY PROTECTION FOR PRIVATE INSURERS WHO SHARE INFORMATION FOR ANTI-FRAUD ENFORCEMENT PURPOSES

Effective detection and investigation of health care fraud often depends on the free flow of health care fraud-related information among private insurers, regulatory agencies, and law enforcement. However, on grounds such as defamation, invasion of privacy, and malicious prosecution, information sharing can expose private insurers to potential civil tort liability. To promote information sharing in investigations, some states have enacted comprehensive immunity statutes protecting health insurers who disclose information for legitimate anti-fraud purposes.

9. Does your state have a statute(s) that requires private insurers to disclose fraud-related information?

1 26 No

2 24 Yes --> 9a. With whom? *(Mark all that apply.)*

1 12 State law enforcement authorities
2 22 State insurance commissioner
3 9 Federal law enforcement authorities
4 5 Federal insurance regulatory agencies
5 3 National Association of Insurance Commissioners
6 1 Other insurers
7 5 Other *(Please specify)* _____

_____

_____

10. Does your state have a statute(s) that provides private insurers with immunity from civil liability for fraud-related information disclosures?

1 38 Yes --> 10a. Please cite the applicable statute(s): _____

_____

_____

*(**Continue with question 11**.)*

2 12 No --> 10b. Do you believe such a statute is needed?

1 7 Yes
2 0 No

*(**Skip to question 16**.)*

11. With which of the following entities does the state's immunity statute(s) allow private insurers to share information? *(Mark all that apply.)*

1 _26_ State law enforcement authorities
2 _37_ State insurance commissioner
3 _25_ Federal law enforcement authorities
4 _10_ Federal insurance regulatory agencies
5 _16_ National Association of Insurance Commissioners
6 __8_ Other insurers
7 __6_ Other *(Please specify)* _____

12. Which of the following qualifiers, if any, does your state's immunity statute(s) place on the provision of immunity? *(Mark all that apply.)*

1 _33_ Absence of malice
2 _23_ Absence of bad faith
3 _20_ Absence of fraudulent intent
4 __5_ Other qualifiers *(Please specify)* _____

_____

5 __0_ No qualifiers

13. Are you aware of any positive effects from your state's immunity law(s) on anti-fraud enforcement efforts?

1 _11_ No

2 _24_ Yes --> 13a. What have been the effects? *(Mark all that apply.)*

1 _16_ Increased information sharing
2 __5_ Reduced investigative duplication
3 _21_ Increased referrals of suspected fraud
4 _14_ Increased number of fraud cases investigated
5 __7_ Expedited investigative/prosecutive efforts
6 __6_ Resulted in stronger court cases
7 __3_ Resulted in harsher sanctions or penalties
8 __2_ Other *(Please specify)*_____

_____

14. Are you aware of any negative effects from your state's immunity law(s) on anti-fraud enforcement efforts?

1 _32_ No

2 __3_ Yes --> 14a. What have been the effects? *(Mark all that apply.)*

1 __1_ Excessive sharing of questionable intelligence
2 __2_ Increased workload of case referrals
3 __0_ Damaged providers' reputations
4 __2_ Other *(Please specify)*_____

_____

7

15. How adequate or inadequate is your state's immunity statute(s) in...

a. protecting private health insurers from civil liability claims?

1 16 Fully adequate
2 8 Somewhat adequate
3 3 Not at all adequate

b. facilitating information sharing with law enforcement authorities?

1 18 Fully adequate
2 8 Somewhat adequate
3 2 Not at all adequate

16. How reluctant are private health insurers to share fraud-related information with...

a. your office?

1 3 Very reluctant
2 20 Somewhat reluctant
3 18 Not at all reluctant

b. other state insurance investigative entities (if applicable)?

1 1 Very reluctant
2 6 Somewhat reluctant
3 11 Not at all reluctant

4 26 No basis for opinion

c. state/local law enforcement entities?

1 2 Very reluctant
2 9 Somewhat reluctant
3 6 Not at all reluctant

4 28 No basis for opinion

d. federal regulatory entities?

1 2 Very reluctant
2 2 Somewhat reluctant
3 4 Not at all reluctant

4 37 No basis for opinion

e. federal law enforcement entities?

1 2 Very reluctant
2 3 Somewhat reluctant
3 5 Not at all reluctant
4 35 No basis for opinion

f. other private insurers investigating health care fraud?

1 11 Very reluctant
2 2 Somewhat reluctant
3 6 Not at all reluctant

4 26 No basis for opinion

8

17. In your opinion, how effective or ineffective would a federal preemptive immunity statute be in facilitating the sharing of fraud-related information in your state...

a. between private health insurers and federal/state law enforcement authorities?

1 14 Very effective
2 19 Somewhat effective
3 6 Not at all effective

17a1. Please explain your answer.

_____

_____

_____

b. between private health insurers and federal/state regulatory authorities?

1 15 Very effective
2 17 Somewhat effective
3 6 Not at all effective

17b1. Please explain your answer.

_____

_____

_____

c. between two or more private health insurers?

1 15 Very effective
2 12 Somewhat effective
3 9 Not at all effective

17c1. Please explain your answer.

_____

_____

_____

9

IV. A CENTRAL DATA REPOSITORY FOR HEALTH CARE FRAUD INFORMATION

Health care fraud schemes often involve the use of sophisticated computer techniques, complicated business arrangements, and multiple locations across state lines. As a result, many health insurers and law enforcement agencies coordinate their enforcement efforts and are exploring methods for collecting, processing, and disseminating health care fraud information throughout the insurer and enforcement communities. The United States Congress has recently considered several proposals relating to the establishment of a centralized health care fraud database. However, the proposals differed in terms of what type of information would be included in the database, who would manage the database, and who would have access to the information in the database.

18. In calendar year 1994, which of the following methods, if any, did your office use to obtain information when investigating health care fraud cases? *(Mark all that apply.)*

1 _22_ Direct contact with health care providers
2 _27_ Direct contact with health insurers
3 _15_ Direct contact with insurance industry groups
4 _21_ Direct contact with state regulatory agencies
5 _20_ Direct contact with state law enforcement agencies
6 _16_ Direct contact with federal regulatory agencies
7 _19_ Direct contact with federal law enforcement agencies
8 __5_ Computerized health care database
9 _12_ Computerized insurance industry database
10 _10_ Computerized law enforcement database

11 _19_ Office did not investigate health care fraud in calendar year 1994 --> *(**Skip to question 27**.)*

19. In calendar year 1994, which of the following types of computerized databases, if any, did your office use during health care fraud investigations? *(Mark all that apply.)*

1 _16_ Internal agency database
2 _13_ State government database
3 __6_ Federal government database
4 _17_ Industry or Association database
5 _12_ Private insurer database
6 __3_ Other *(Please specify)*_____

_____

_____

7 __6_ Office did not use any computerized databases during health care fraud investigations. --> *(**Skip to question 21**.)*

20. When investigating health care fraud cases in calendar year 1994, from which of the following databases did your office request information? *(Mark all that apply.)*

1 __5__ the Provider Indexing Network System (PINS)

20a. How useful was the information?

1 __2__ Very useful
2 __3__ Useful
3 __0__ Not very useful

2 __0__ the National Practitioner Data Bank (NPDB)

20b. How useful was the information?

1 __0__ Very useful
2 __0__ Useful
3 __0__ Not very useful

3 _16_ the National Association of Insurance Commissioners (NAIC)

20c. How useful was the information?

1 __8__ Very useful
2 __6__ Useful
3 __2__ Not very useful

4 _18_ the National Insurance Crime Bureau (NICB)

20d. How useful was the information?

1 __7__ Very useful
2 __8__ Useful
3 __3__ Not very useful

5 __1__ the Financial Crimes Enforcement Network (FinCEN)

20e. How useful was the information?

1 __1__ Very useful
2 __0__ Useful
3 __0__ Not very useful

6 _12_ the National Crime Information Center (NCIC)

20f. How useful was the information?

1 __8__ Very useful
2 __3__ Useful
3 __1__ Not very useful

7 __1__ Office did not request information from any of these databases during calendar year 1994.

11

21. In your opinion, would a central repository of health care fraud-related information facilitate health care fraud enforcement efforts?

1 __2__ No --> 21a. If no, why not? *(Mark all that apply.)*

1 __1__ Information is available from other sources
2 __1__ Local focus would be more useful than national
3 __2__ Access restrictions might limit usefulness
4 __0__ Other *(Please specify)* _____

_____

_____

*(**Skip to question 27**.)*

2 __26__ Yes --> 21b. In what ways? *(Mark all that apply.)*

1 __22__ Reduce investigative duplication
2 __23__ Expedite enforcement actions
3 __15__ Strengthen prosecutions
4 __12__ Lead to harsher penalties
5 __5__ Other *(Please specify)* _____

_____

_____

22. In your opinion, would there be any negative effects of a central health care fraud repository?

1 __11__ No

2 __18__ Yes --> 22a. If yes, which of the following could be negative effects? *(Mark all that apply.)*

1 __12__ Lack of security/confidentiality
2 __11__ Improper use of information
3 __13__ Inaccurate information
4 __8__ Costly to operate
5 __1__ Other *(Please specify)* _____

_____

_____

23. In your opinion, at what level should a central health care fraud repository be established? *(Mark one.)*

1 __10__ Federal government
2 __8__ State government
3 __7__ Private sector
4 __4__ Other (Please specify) _____

_____

_____

12

24. In your opinion, to enhance health care fraud enforcement efforts, how important or unimportant is it for a central health care fraud repository to contain information about...

a. suspected fraud referrals?

1 22 Very important
2 6 Somewhat important
3 0 Not at all important

b. investigative activities (such as intelligence and leads)?

1 21 Very important
2 7 Somewhat important
3 1 Not at all important

c. ongoing investigations?

1 22 Very important
2 7 Somewhat important
3 0 Not at all important

d. final adverse actions taken?

1 27 Very important
2 2 Somewhat important
3 0 Not at all important

25. In your opinion, to enhance health care fraud enforcement efforts, how important or unimportant is it for the following entities to be able to input information into a central health care fraud repository?

a. State regulatory agencies

1 28 Very important
2 1 Somewhat important
3 0 Not at all important

b. State law enforcement agencies

1 28 Very important
2 1 Somewhat important
3 0 Not at all important

c. Federal regulatory agencies

1 27 Very important
2 2 Somewhat important
3 0 Not at all important

d. Federal law enforcement agencies

1 29 Very important
2 0 Somewhat important
3 0 Not at all important

e. Private insurance companies

1 25 Very important
2 3 Somewhat important
3 1 Not at all important

13

26. In your opinion, to enhance health care fraud enforcement efforts, how important or unimportant is it for the following entities to be able to retrieve information from a central health care fraud repository?

a. State regulatory agencies

1 27 Very important
2 1 Somewhat important
3 1 Not at all important

b. State law enforcement agencies

1 26 Very important
2 3 Somewhat important
3 0 Not at all important

c. Federal regulatory agencies

1 21 Very important
2 7 Somewhat important
3 1 Not at all important

d. Federal law enforcement agencies

1 25 Very important
2 4 Somewhat important
3 0 Not at all important

e. Private insurance companies

1 17 Very important
2 8 Somewhat important
3 3 Not at all important

27. If you have any other comments related to health care fraud enforcement issues, please write them in the space below. If you need more space, attach a separate sheet.
(*We may telephone you to obtain additional information.*)

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

15

Databases and Other Information Resources That May Be Useful to Health Care Fraud Investigators

Federal Resources

National Crime Information Center

The National Crime Information Center is the nation's most extensive computerized criminal justice information system. The system consists of a central computer at FBI headquarters in Washington, D.C.; dedicated telecommunications lines; and a coordinated network of federal and state criminal justice information systems. The system provides users with access to over 24 million records in 14 files, such as files on wanted persons, stolen vehicles, and missing persons. The system's largest file, the Interstate Identification Index, provides access to about 17 million criminal history information records contained in state systems.

Over 19,000 federal, state, and local law enforcement and other criminal justice agencies in the United States and Canada can access the National Crime Information Center directly. About 97,000 computer terminals in these agencies can access the system. An additional 51,000 law enforcement and other criminal justice agencies can access the system indirectly through agreements with user agencies that have direct access. More than 500,000 individuals within the user agencies can access the system, either directly from their own computer terminals or indirectly through computer terminal operators.

The FBI is responsible for overall management of the National Crime Information Center. However, an Advisory Policy Board, composed of managers of state and local user systems, is responsible for establishing and implementing operational policies, including security.

HHS Sanctions

HHS has the authority to exclude from participation in the Medicare and Medicaid programs any health care providers and practitioners determined to have engaged in fraudulent or abusive practices. Under section 1128(a) of the Social Security Act, exclusion is mandatory for program-related convictions and for patient abuse or neglect convictions. Section 1128(b) of the act lists 14 bases upon which HHS has permissive or optional authority to make exclusions. These exclusion bases include, for example, fraud-related convictions, license revocations or suspensions by state boards,[1] and defaults on health education loan obligations. During fiscal years 1990 through 1995, HHS reported that it excluded 6,986 providers and practitioners from the Medicare and Medicaid programs.

[1]According to HHS Office of Inspector General officials, the agency routinely obtains reports (of license revocations and suspensions) from the National Federation of State Licensing Boards.

HHS makes the names of excluded providers and practitioners available through various channels. Twice a year, for example, the HHS Office of Inspector General prepares a Cumulative Sanction Report, which is an alphabetical listing of excluded individuals and entities. For each name listed, the report shows date of birth (for individuals), health care specialty, address, and basic information on the exclusion (type of action, date of notice, and length of the exclusion period). Upon request, HHS provides the report (a paper copy or downloaded to a diskette) to interested parties. Also, beginning in fall 1995, HHS made the list of excluded providers and practitioners accessible via Internet. Further, HHS provides monthly exclusion updates to the National Federation of State Licensing Boards.

Health Care Financing Administration's Fraud Investigation Database

The Fraud Investigation Database will be the first nationwide system devoted solely to Medicare fraud and abuse data accumulation. In January 1996, the Health Care Financing Administration field tested the system and plans to have it fully operational later in the year. As currently planned, the system will provide the current status of all Medicare fraud cases, a chronology of events, and documentation of those cases referred to law enforcement agencies. Organizations with access to the system will include Health Care Financing Administration central and regional offices, Medicare contractors, HHS Office of Inspector General, DOJ, and FBI.

National Practitioner Data Bank

Pursuant to the Health Care Quality Improvement Act of 1986 (Title IV of P.L. 99-660), the National Practitioner Data Bank was created as a clearinghouse for the collection and release of certain information related to the professional competence and conduct of physicians, dentists, and other health care practitioners. The intent of the 1986 act is to improve the quality of health care by (1) encouraging health care practitioners to identify and discipline those engaged in unprofessional behavior and (2) restricting the ability of unethical or incompetent practitioners to move from state to state without disclosure or discovery of their previous damaging or incompetent performance.

The Data Bank is intended to function primarily as a flagging system to facilitate a comprehensive review of professional credentials. The law requires applicable entities to report adverse action information to the Secretary of HHS for inclusion in the Data Bank. Specifically, within 15 days of an adverse action, hospitals, other health care entities, and professional societies must submit reports to the appropriate state

medical or dental boards.[2] In turn, within 15 days these boards are responsible for forwarding the reports to the Data Bank. In addition, with regard to licensure actions—such as revocation or suspension of a physican's or dentist's license—reports to the Data Bank must be submitted by the boards within 30 days of the date such action is taken. Also, within 30 days of a payment, medical malpractice payers must submit reports to the Data Bank and to the appropriate state licensing board. According to HHS guidelines:

"The Data Bank is intended to augment, not replace, traditional forms of credentials review. As a nationwide flagging system, it provides another resource to assist State Licensing Boards, hospitals, and other health care entities in conducting extensive, independent investigations of the qualifications of the health care practitioners they seek to license, hire, or to whom they wish to grant clinical privileges."[3]

In December 1988, HHS' Health Resources and Service Administration awarded a 5-year, $15.8-million contract to the Unisys Corporation to develop and operate the Data Bank at the company's computer facility in Camarillo, California. In September 1990, this national clearinghouse system began operating. The 1986 act allows HHS to charge user fees to recover the costs of processing queries. When the Data Bank first opened, the basic user fee was $2 per query; however, due to higher than expected processing costs, the fee was increased to $6 within the first year of operations. At the time of our review in 1995, the basic fee was still $6 per query.

In general, to be eligible to query the Data Bank, an entity must be (1) a board of medical examiners or other state licensing board, (2) a hospital or other health care entity that provides health care services and engages in formal peer review activity, (3) a professional society that engages in professional review activity through a formal peer review process, or (4) a health care practitioner who requests information concerning himself or herself.[4] The general public may not request information from the Data Bank, except in a form that does not allow identification of a particular person or entity. Also, medical malpractice payers may not request information even though they are required to report.

[2]Adverse actions are defined as adverse licensure actions, adverse clinical privilege actions, and adverse professional society membership actions.

[3]HHS, Health Resources and Service Administration, National Practitioner Data Bank Guidebook, Publication No. HRSA-94-027 (Rockville, MD: October 1994), p. A-3.

[4]Note that the list of entities eligible to query the Data Bank does not include law enforcement agencies. Entities entitled to participate in the Data Bank are defined in provisions of the 1986 Act, as amended, and in regulations codified at 45 CFR Part 60.

As of December 1994, the Data Bank contained reports on more than 97,000 disciplinary/adverse actions or malpractice payments involving almost 73,000 individual practitioners. Of these practitioners, 75.1 percent were physicians, 15.5 percent were dentists, and the remaining 9.4 percent were other health care practitioners. From September 1990 through December 1994, the Data Bank responded to over 4.5 million queries from hospitals, licensing boards, professional societies, and individual practitioners. According to a Health Resources and Service Administration official, responses to Data Bank queries are electronically disseminated to requesters by modem or diskette (about 88 percent) or by mail (about 12 percent).

Financial Crimes Enforcement Network

Established in 1990, the Financial Crimes Enforcement Network (FinCEN) is a separate office within the Department of the Treasury. FinCEN is a governmentwide, multisource intelligence and analytical entity that does not initiate or carry out any investigations on its own. Rather, its primary purpose is to assist other agencies by (1) identifying suspected offenders and reporting on trends and patterns in money laundering by analyzing various databases maintained by other agencies, (2) developing and disseminating research and policy studies on money laundering enforcement, (3) supporting governmentwide law enforcement by providing tactical support for ongoing investigations, and (4) supporting other law enforcement agencies by using database queries to answer requests for information received at a communications center.

Currency transaction and other reports required by the Bank Secrecy Act (P.L. 91-508, 84 Stat. 1114) are the primary source for most of the financial intelligence information accessed and disseminated by FinCEN staff. Generally, by accessing and researching various databases, FinCEN analysts uncover and piece together information about (1) bank accounts, bearer bonds and other securities, real property, vehicles, and other assets; (2) accomplices, known associates, additional suspects, and witnesses; and (3) Social Security numbers, birth dates, addresses, phone numbers, and other identifying items.

State Resources

National Association of Insurance Commissioners

As the nation's oldest association of state officials, the National Association of Insurance Commissioners coordinates the insurance

regulatory efforts of the various states. The Association maintains the largest insurance industry database in the world. The database contains information from the annual financial statements of more than 5,000 U.S. insurers—which represent about 99 percent of all U.S.-based insurance companies. The database provides state insurance commissioners and state departments of insurance with the information needed to regulate and monitor the solvency of insurance companies, among other things.

The database also contains a synopsis of formal regulatory or disciplinary actions—cease and desist orders, license revocations and suspensions, fines and penalties, etc.—taken against insurance agents and companies. Available on-line since 1988, this information can be searched routinely by regulators to help prevent violations in multiple jurisdictions. Search options include Social Security numbers, dates of birth, and company codes; also, reports may be generated for any given date range.

In 1990, the database's regulatory and disciplinary action information became available to the public. For example, according to Association literature, insurers can purchase the information to screen applicants for agent licensure purposes and to identify current agents. In 1994, more than 12,800 new actions were added to the database. As of 1995, the database contained the names of more than 50,000 insurance agents and companies against which some regulatory actions have been taken. Also, during 1995, this database information became available to regulators and insurers in a CD-ROM format.

Industry and Commercial Resources

Provider Indexing Network System

The Provider Indexing Network System is a database that enables NHCAA corporate members and participating public sector organizations (including the FBI and the HHS Office of Inspector General) to share information on health care fraud and possibly combine investigative cases in order to make them prosecutable at the federal level. Information in the database includes (1) the names and full business identities of providers suspected, indicted, or convicted of health care fraud; and (2) a description of the specific types of fraudulent activity involved. According to NHCAA officials, data are entered into the system only if the information

pertains to (1) an actual ongoing fraud investigation by a member company, (2) a fraud-related criminal indictment, or (3) a fraud conviction. Further, an Association official told us that beginning in 1994, the system began to include data on sanctions imposed by HHS on Medicare and Medicaid providers.

The database is located at NHCAA headquarters in Washington, D.C. It is a bulletin board system with on-line, password-protected data-input and data-retrieval access available to authorized users by telephone modem. Users can focus or customize access queries to obtain, for example, information involving a specific health care specialty, a certain type of fraud, or a given geographic area.

National Insurance Crime Bureau

The National Insurance Crime Bureau is a nonprofit organization supported by approximately 1,000 property/casualty insurers and self-insured companies for the purpose of actively assisting law enforcement. Among the Crime Bureau's goals are to (1) promote deterrence and prevention of insurance crimes by working with the public, law enforcement, insurance departments, and elected officials; and (2) provide a single information-sharing network to optimize insurance crime investigation, prosecution, and restitution.

As a tool to enhance investigative effectiveness, the Crime Bureau maintains an interactive database containing comprehensive insurance claim and vehicle-related information, such as automobile theft and accident claims and workers' compensation claims. The database is continually updated with records provided by insurance companies, self-insured companies, vehicle manufacturers, impound lots, shipping lines, state fraud bureaus, law enforcement agencies, and the U.S. Customs Service. The Crime Bureau also maintains historical stolen vehicle and property records that the FBI has purged from National Crime Information Center files.

Although the Crime Bureau's database contains information primarily involving property/casualty and automobile insurance fraud, there is often a health care fraud component to such fraud. For example, staged automobile accidents often are designed to generate fraudulent bodily injury claims. Furtherance of these schemes requires the knowing participation of health care providers to falsely document injuries. The identity of these providers is important intelligence for insurance fraud

investigators because unethical providers are often involved in many fraud schemes simultaneously.

Comments From the National Health Care Anti-Fraud Association

NHCAA NATIONAL HEALTH CARE ANTI-FRAUD ASSOCIATION
1255 Twenty-Third Street, NW ■ Washington, DC 20037-1174 ■ (202) 659-5955 ■ Fax (202) 833-3636

March 29, 1996

Norman J. Rabkin
Director, Administration of
Justice Issues
United States General Accounting Office
Washington, DC 20548

Dear Mr. Rabkin:

Enclosed, in response to your letter of February 26, are the formal comments of the National Health Care Anti-Fraud Association (NHCAA) on GAO's draft report entitled Health Care Fraud: Information-Sharing Proposals to Improve Enforcement Efforts.

We also have sent a copy this afternoon via facsimile to Dan Burton and Philip Caramia of GAO's Dallas office.

On behalf of NHCAA, we appreciate this and the previous fine work that GAO has performed in examining and reporting on health care fraud during the last several years.

Thank you very for GAO's interest in obtaining NHCAA's perspective on these issues and for giving us the opportunity to comment on the draft report.

Please contact me should you have any questions or require any further information—or whenever NHCAA might be of assistance in the future.

Sincerely yours,

William J. Mahon
Executive Director

enclosures

cc: NHCAA Executive Committee

T393C

COMMENTS

OF THE

**NATIONAL HEALTH CARE
ANTI-FRAUD ASSOCIATION**

on

**GAO Draft Report
"Health Care Fraud: Information-Sharing
Proposals to Improve Enforcement Efforts"**

March 29, 1996

The National Health Care Anti-Fraud Association ("NHCAA") appreciates the opportunity to comment on the draft report discussing a potential federal immunity statute for the reporting of information concerning suspected health insurance fraud and the possible creation of a federal database for information concerning health insurance fraud. NHCAA wholeheartedly endorses the idea of a federal immunity statute. In addition, the database, if it contains complete information with appropriate access for public and private payers, can be an excellent supplemental tool for fighting health care fraud.

As indicated in the draft report, creating a federal immunity statute will play a significant role in expanding the private sector's ability to participate in the fight against health care fraud, both in initiating investigations and providing cooperation to law enforcement. Today, when insurers or other private parties participate in the investigation of criminal fraud, whether on their own initiative or in cooperation with law enforcement officials, they risk civil liability (e.g., defamation, invasion of privacy, malicious prosecution) to the targets of these investigations—typically affluent, sophisticated health care practitioners whose entire livelihood may be in jeopardy. The threat of costly civil litigation and the limited (but very real) risk of substantial open-ended punitive damage awards discourages some insurers from active anti-fraud programs.

Immunity statutes are one important means of alleviating these threats and encouraging private payers to cooperate aggressively with law enforcement to fight fraud. The current state-based immunity structure, while useful, is insufficient to protect fully those who come forward with information about suspected health care fraud. As the draft report notes, immunity statutes exist only in a limited number of states. The statutes that are in effect vary significantly by state, with some states providing strong immunity for good-faith participation in fraud investigations and others providing limited or no realistic immunity. Where immunity protection is not available or effective, private payers understandably may be reluctant to fully participate in fraud investigations or to share information on these investigations with others who may be victims of the same or similar schemes.

In addition, the state-based structure does not recognize the modern reality of health care fraud investigation and detection. Many fraud schemes simply do not confine themselves to state boundaries. Regional and even national schemes are becoming commonplace, as recognized both by the increased federal involvement in health fraud investigations and the increasing effort to develop additional federal anti-fraud legislation. Accordingly, a federal immunity statute is needed to protect effectively private payers that participate in these multi-state fraud investigations. NHCAA firmly believes that a federal immunity statute will play a significant role in expanding the role of private payers in fighting health care fraud.

In addition to this "encouragement" function of immunity statutes, a federal immunity statute, particularly if it protects insurer-to-insurer communication, will create the opportunity for the more effective development of health care fraud cases. Dishonest providers rarely defraud only one payer at a time—indeed the safest approach (and the most lucrative) is to defraud multiple payers simultaneously and in less conspicuous increments. Similarly, almost never do dishonest providers defraud either the private or public sector exclusively: Experience shows that the provider who defrauds Medicare, Medicaid, CHAMPUS or other government programs in all likelihood also defrauds private insurers, and vice-versa. Because there are multiple victims, fraud cases are most effectively detected and investigated through group activity, by cooperative sharing of information among private payers and with law enforcement. An immunity statute that protects such sharing of investigative efforts will allow public and private payers to combine their efforts to better detect fraud. In addition, with the limited enforcement resources at all levels of law enforcement, allowing the sharing of investigative information results in bringing larger and more complete investigations to law enforcement, to put those limited law enforcement resources to better use.

The immunity legislation must be drafted in a way that effectively serves these joint goals of encouraging the communication of information and building better cases. The immunity "model" from S. 1088 (discussed in the draft report) has been included, with some variations, in virtually all anti-fraud proposals introduced in the past three years, far beyond the proposals identified in the draft report. Inclusion of this immunity in a larger anti-fraud package is particularly important because many of the anti-fraud legislative proposals require payers to provide certain information.

The immunity concept embodied in S. 1088 and the original Clinton health care reform plan is a good one. To facilitate this crucial exchange of information, insurers must have effective protection from tort suits for good faith participation in fraud investigations. To provide qualified immunity for certain information disclosures under the federal anti-fraud program, these bills incorporate the immunity provisions of the Social Security Act, by stating that persons providing information to particular law enforcement officials "in conjunction with their performance of duties" will receive this qualified immunity.

This federal-level immunity would be an important step forward. Under the Social Security Act, no persons providing information shall be held "to have violated any criminal law, or to be civilly liable under any law" unless they have provided information unrelated to their performance of duties or unless the information was false and the person providing information "knew, or had reason to believe, that such information was false." 42 U.S.C. § 1320c-6.

Although limited in its protection, the recognition of the need for uniform federal protection is important. Nonetheless, there are a few important issues to resolve, to make this immunity protection fully effective.

First, protection should be afforded to all anti-fraud investigative activities, not just those involving the "performance of duties" under a federal anti-fraud program. The draft GAO report broadly interprets the language of these statutory proposals. However, it must be made clear that providing information in the context of any health care fraud investigation will be protected. This is particularly important because some of the pending reform proposals do not include private sector health claims in the scope of the coordinated fraud program to be put together by the Attorney General and the Secretary of Health and Human Services. Restricting the protection to "performance of duties" under the program therefore provides a roadmap on how to evade this immunity, and will create unnecessary and distracting litigation disputes that will defeat the purpose of providing immunity.

The immunity should also extend to the provision of information to all law enforcement officers, not just those connected to the administration of the health care system, to encourage cooperation with these law enforcement officials wherever appropriate. It makes little sense to provide immunity for disclosures to the U.S. Attorney, but not to a state prosecutor or a Postal Inspector.

Moreover, given the private sector's critical role in health care fraud investigations, it is crucial for this immunity to apply to exchanges of information between private sector fraud investigators, as the private sector investigators often are the first line of defense against fraud. It is this insurer-to-insurer communication that will allow for the development of larger, more complete cases that will maximize the efficiency of law enforcement efforts.

In addition, while NHCAA recognizes that this immunity likely will not be absolute,[1] the exception in the statutory proposal for provision of false information must not prove to be a significant loophole. The Cohen proposal, for example, revokes immunity protection where the person providing false information "knew, or had reason to believe, that [the] information was false." In these instances, the mere allegation in a complaint of "falsity" could be sufficient to remove the immunity. This immunity standard should be strengthened, by requiring that any allegation of knowledge of false information be required to be

[1] The Annuzio-Wylie Anti-Money Laundering Act of 1992, cited in the draft report at footnote 32, provides complete immunity for a "financial institution that makes a disclosure of any possible violation of law. . . ." Accordingly, there is federal statutory precedent for absolute immunity in this context.

pled "with particularity," a term of art under the Federal Rules of Civil Procedure, Rule 9(b), so that there must be allegations of specific behavior beyond that normally required in a complaint. In addition, as with some state immunity laws like the one in New Hampshire, attorneys fees should be awarded to a payer that is sued that is found to be entitled to immunity.

On the whole, the legislative proposals to date make a significant step forward in creating some level of federal immunity protection. However, because the participation of private payers is critical to effective fraud investigations, this participation must be encouraged by broader immunity protection. Particularly in an environment where public law enforcement is dedicating additional resources to fighting fraud in public programs, allowing private payers a more effective means of sharing information and cooperating with law enforcement will be a significant step forward in the fight against health care fraud. NHCAA therefore strongly supports the adoption of an effective federal immunity statute.

In addition to the proposed immunity statute, the draft report also addresses the creation of a database of information concerning health care fraud. If properly created, this database would provide a useful additional tool in fighting health care fraud.

The GAO report uses the NHCAA Provider Indexing Network System ("PINS") as one example of a similar database. There are certain corrections that should be made to the description of this system. The "PINS" system is available to NHCAA member companies and participating law enforcement agencies, all of whom must agree to abide by the procedures established for submission of data to PINS and use of information obtained from PINS. These procedures govern when and what type of information can be submitted to PINS, how this data is to be updated, when inquiries can be made of PINS and what limited uses can be made of PINS data. As of March, 1996, the system contains 1,984 records.

In general, PINS data in and of itself is not "evidence" of any kind of fraudulent activity, and instead represents merely a means of focusing limited investigative resources, in each organization's independent discretion. Every private payer that participates in the PINS system agrees to indemnify the other PINS participants if liability results from its misuse of PINS data.

NHCAA has found the PINS system to be a useful adjunct to an active, ongoing anti-fraud operation. The experience with PINS indicates that a database of this kind will be most useful when it includes active investigations, where the safeguards and procedures for use of the database are carefully outlined and where the costs of such a database are modest.

If these provisions are incorporated, and appropriate access is provided to private sector payers, this kind of database can be an effective fraud-fighting tool. This database will be particularly helpful if there is disclosure of information by both law enforcement agencies and private payers on a regular basis.

Finally, with respect to the private-public makeup of NHCAA, the organization now numbers 70 private-sector corporate members (comprising commercial and not-for-profit health insurers, a major third-party-administrator firm and a major self-insured corporation) and public-sector participants from the Offices of Inspector General at the U.S. Departments of Defense, Health & Human Services, Labor, Veterans Affairs and the Office of Personnel Management; the Health Care Financing Administration; the criminal investigations division of the U.S. Postal Inspection Service; and the National Association of Medicaid Fraud Control Units.

NHCAA also maintains formal "Law Enforcement Liaison" relationships with the U.S. Department of Justice, the Federal Bureau of Investigation, the U.S. Federal Trade Commission—Bureau of Consumer Affairs, and the Criminal Investigations Division of the Internal Revenue Service.

NHCAA also numbers more than 800 Individual Members from the ranks of those private- and public-sector organizations and from other health insurance companies, self-insured corporations and federal and state agencies.

Again, NHCAA appreciates the opportunity to participate in this important GAO undertaking and will be pleased to provide any further assistance.

P005

Comments From the American Medical Association

American Medical Association
Physicians dedicated to the health of America

P. John Seward, MD
Executive Vice President

515 North State Street
Chicago, Illinois 60610

312 464-5000
312 464-4184 Fax

March 19, 1996

Mr. Norman J. Rabkin
Director, Administration of Justice Issues
General Government Division
General Accounting Office
Washington, DC 20548

Dear Mr. Rabkin:

On behalf of its 300,000 physician and medical student members, the American Medical Association (AMA) thanks you for the opportunity to comment on the draft report of the General Accounting Office (GAO) entitled, "Health Care Fraud: Information-Sharing Proposals to Improve Enforcement Efforts." The AMA deplores all fraudulent and abusive schemes that undermine health care delivery and increase the cost of health care in this country. For years, the medical community and health insurers have struggled to find the best and most efficient method of tracking and prosecuting individuals who commit health care fraud. Granting immunity to those who report health care fraud-related information and creating a national fraud database are two efforts that many have proposed to curb this abhorrent practice.

In crafting a solution to fraud and abuse in both the private and public health care markets, the AMA believes it is essential to understand the precise dimensions of the problem. Without this basic understanding, legislative efforts to curb fraud and abuse may be misdirected and unsuccessful. As the draft GAO report recognizes, solutions to the fraud and abuse problem present an inherent conflict between dual public policy goals: supporting the investigation and prosecution of fraud; and protecting innocent people against unsubstantiated allegations made in bad faith or with malice.

The GAO draft report focuses on two information-sharing issues that are being considered in various legislation pending before Congress: (1) granting immunity to those who report health care fraud information; and (2) a national, centralized health care fraud database. The question is would these suggested improvements enhance existing enforcement mechanisms in combatting health care fraud. Our comments address this issue.

I. Federal Immunity for Reporters of Health Care Fraud

The AMA supports the need for agencies to access information regarding those who engage in health care fraud and abuse. Granting immunity from liability to those who report fraudulent acts committed by health care providers and practitioners could

arguably increase and improve law enforcement's ability to access such information. The draft GAO report recognizes that most states have enacted immunity laws that protect insurers that share health care fraud information. Legislation pending before Congress would grant immunity to health plans that share information among each other and expand such protection to any individual who reports fraudulent and abusive behavior.

In general, the AMA supports immunity for reporting fraudulent practices in the health care arena because it assists law enforcement efforts to bring perpetrators to justice. This in turn will presumably lower health care costs and improve the quality of the health care delivered. That said, medical information, by its nature, is sensitive and private. Any legislation that grants immunity for insurers and any other entities to share information regarding suspected fraudulent behavior should include safeguards to ensure that such information is not used inappropriately. For example, an insurance company may share information with another insurer about a physician whose medical practice the company finds suspicious. Based on this unsubstantiated claim alone, the receiver of this information could decide to "deselect" the physician, and that physician then may not be able to find another plan with which to associate.

For immunity to have the intended benefit (i.e. to encourage more truly fraudulent behavior to be reported), the shared information must be related to specific conduct. And the conduct must be outside the realm of legitimate disagreements on what care is medically necessary. In addition, there must be some substantiation of the information, so that its credibility is not in question. Moreover, a person who shares false information, knowing that it is false, should not be immune from liability. There must be an opportunity for one who is harmed by "bad faith" sharing of information to seek legal recourse. If immunity is provided to those who report health care fraud, a remedy must be afforded the accused individual against bad faith allegations that could detrimentally affect his or her reputation and livelihood.

II. Establishment of a Centralized Database

The second part of the GAO draft report examines the necessity for and potential effectiveness of a centralized database which would contain health care fraud and abuse information on the part of providers and practitioners. As with the immunity provision, most fraud and abuse bills before Congress contain some version of such a database. The purpose of the database is to share information related to fraud and abuse by health care providers among federal, state and local enforcement agencies. Most databases would contain "final adverse actions" against providers and practitioners. This would include civil judgments, criminal convictions, revocation or suspension of a license, and any other negative action or finding against a practitioner. Depending on the particular database, this information is reported to

various government agencies and may be available to health plans and, in some cases, to the public.

Although the AMA supports the sharing of information related to fraud and abuse, we believe that creating a national database at this time may not be the best use of limited enforcement dollars, particularly since the information that would be contained in the database is already publicly available from other sources. Databases can be exceedingly expensive to establish and maintain. The National Practitioner Databank (NPDB) is a perfect example. Since it became operational in 1990, the NPDB has cost more than $23 million to establish and operate. This databank, however, contains more limited information than the databases contemplated in legislation pending before Congress. Therefore, it is not unreasonable to expect that the cost of a centralized national database would far exceed the $5.8 million it costs per year to operate the NPDB.

In addition, there could be problems with inappropriate use and disclosure of information contained in the database. For instance, the information could mistakenly identify and target an individual provider who has not violated any law. Moreover, most databases would contain any and all "final adverse actions," even those totally unrelated to fraud. Thus, an individual's speeding ticket or parking fine could end up in the database. The utility of this kind of information is highly questionable.

The AMA is also mindful that maintaining security over the information in the database would be difficult. With potentially thousands of people having access to information in the database, ensuring that information regarding patient records are not divulged would be next to impossible. In our experience, most databases fail to adequately protect the confidentiality of patitent records.

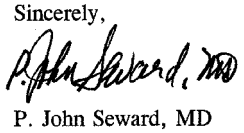
III. Conclusion

The AMA would support granting immunity to those reporting incidents of health care fraud, provided adequate safeguards are established so that the nature of the conduct reported is specific. Information regarding a physician's medical decision making and treatment decisions must not be grounds for accusations of fraud. In addition, any allegation of fraudulent behavior must be sufficiently substantiated. Finally, there must be legal recourse for "bad faith" or malicious reporting.

The AMA believes that at this time a centralized database may not be the best use for limited enforcement resources. There are many problems inherent in establishing and maintaining such a database. It is exceedingly costly; there is great potential for the inappropriate use and disclosure of information contained in the data base; and most data bases do not sufficiently protect the confidentiality of patient records.

The AMA appreciates the opportunity to comment on these two information-sharing techniques. We are committed to routing out fraudulent and abusive behavior wherever it exists, and we look forward to working together on this very important issue.

Sincerely,



P. John Seward, MD

Major Contributors to This Report

General Government Division, Washington, D.C.	David P. Alexander, Senior Social Science Analyst Pamela V. Williams, Communications Analyst
Office of the General Counsel	Jan B. Montgomery, Assistant General Counsel
Dallas Field Office	Danny R. Burton, Assistant Director Philip D. Caramia, Senior Evaluator Warren M. Lundy, Evaluator Frederick T. Lyles, Evaluator Dorothy M. Tejada, Computer Specialist Beth D. Atkins, Technical Information Specialist

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. VISA and MasterCard credit cards are accepted, also. 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 (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100

Official Business
Penalty for Private Use $300

Address Correction Requested