United States Government Accountability Office

GAO

Report to Congressional Committees

September 2006

PRIVACY

Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid, and TRICARE

GAO-06-676

September 2006

PRIVACY

Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid, and TRICARE

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-06-676, a report to congressional committees

Why GAO Did This Study

Federal contractors and state Medicaid agencies are responsible for the day-to-day operations of the Medicare, Medicaid, and TRICARE programs. Because these entities may contract with vendors to perform services involving the use of personal health data, outsourcing and privacy protections are of interest. GAO surveyed all federal Medicare and TRICARE contractors and all state Medicaid agencies (a combined total of 378 entities) to examine whether they (1) outsource services—domestically or offshore—and (2) must notify federal agencies when privacy breaches occur. Survey response rates ranged from 69 percent for Medicare Advantage contractors to 80 percent for Medicaid agencies. GAO interviewed officials at the Department of Health and Human Services' Centers for Medicare & Medicaid Services (CMS), which oversees Medicare and Medicaid, and the Department of Defense's TRICARE Management Activity (TMA), which oversees TRICARE.

What GAO Recommends

Similar to the requirements that currently apply to TRICARE and Medicare FFS contractors, GAO recommends that CMS require state Medicaid agencies and all Medicare contractors responsible for safeguarding personal health information to notify CMS of privacy breaches. In their comments, CMS concurred with our recommendation and DOD concurred with our findings on TRICARE.
www.gao.gov/cgi-bin/getrpt?GAO-06-676.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Leslie G. Aronovitz at (312) 220-7600 or aronovitzl@gao.gov .

What GAO Found

Federal contractors and state Medicaid agencies widely reported domestic outsourcing of services involving the use of personal health information but little direct offshore outsourcing. Among those that completed GAO's survey, more than 90 percent of Medicare contractors and state Medicaid agencies and 63 percent of TRICARE contractors reported some domestic outsourcing in 2005. Typically, survey groups reported engaging from 3 to 20 U.S. vendors (commonly known as subcontractors). One federal contractor and one state Medicaid agency reported outsourcing services directly offshore. However, some federal contractors and state Medicaid agencies also knew that their domestic vendors had initiated offshore outsourcing. Thirty-three Medicare Advantage contractors, 2 Medicare fee-for-service (FFS) contractors, and 1 Medicaid agency indicated that their domestic vendors transfer personal health information offshore, although they did not provide information about the scope of personal information transferred offshore. Moreover, the reported extent of offshore outsourcing by vendors may be understated because many federal contractors and agencies did not know whether their domestic vendors transferred personal health information to other locations or vendors.

In responding to GAO's survey, over 40 percent of the federal contractors and state Medicaid agencies reported that they experienced a recent privacy breach involving personal health information. (The frequency or severity of these breaches was not reported.) By survey group, 47 percent of Medicare Advantage contractors reported privacy breaches within the past 2 years, as did 44 percent of Medicaid agencies, 42 percent of Medicare FFS contractors, and 38 percent of TRICARE contractors. TMA and CMS differ in their requirements for notification of privacy breaches. TMA requires monthly reports on privacy breaches from its TRICARE contractors and follows up with contractors that report recurring lapses in privacy. While CMS requires Medicare FFS contractors to report privacy breaches within 30 days of discovery, such oversight is lacking for privacy breaches that may occur with personal health information held by state Medicaid agencies and Medicare Advantage contractors, as CMS does not require reports of privacy breaches from these entities.

Contents

Abbreviations

CMS	Centers for Medicare & Medicaid Services
EU	European Union
FFS	fee-for-service
HIPAA	Health Insurance Portability and Accountability Act
TMA	TRICARE Management Activity

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

September 5, 2006

Congressional Committees

Private firms that contract with federal agencies, as well as state Medicaid agencies, play a lead role in administering three of the nation's largest public health insurance programs—Medicare, Medicaid, and the Department of Defense's TRICARE program.[1] These federal contractors and state Medicaid agencies carry out the day-to-day operations of their respective health programs by performing a variety of services, such as enrolling people into these programs, processing claims for payment, and operating call centers to assist enrollees. In conducting these activities, the federal contractors and state agencies have access to databases containing personal health information—such as an individual's medical diagnosis, type of provider visited, or use of health care services—on the more than 100 million Americans covered by these programs.

The federal contractors and state Medicaid agencies may contract with other companies—called vendors—to perform specific services routinely or to supplement their staff in times of peak demand. These arrangements—called outsourcing—may involve the disclosure of personal health information to vendors within the United States (domestic outsourcing) or to vendors in other countries (offshore outsourcing).[2] In some cases, the original outsourcing agreement may be followed by one or more subcontracting arrangements known as "downstream" outsourcing.

Questions have been raised about whether outsourcing services involving personal health information increases the vulnerability of such information to improper disclosure. In 2004, patient survey data from a California medical center were inadvertently made available to other

[1]In 2005, Medicare covered about 42 million elderly and disabled individuals and TRICARE covered about 9 million active duty military service members and retirees and their dependents. In 2004, the latest year for which data are available, Medicaid covered about 56 million low-income individuals.

[2]For the purposes of this report, we define offshore outsourcing as providing services that are performed by workers located in foreign countries, whether the workers are employees of U.S. or foreign companies. See GAO, *International Trade: Current Government Data Provide Limited Insight into Offshoring of Services*, GAO-04-932 (Washington, D.C.: Sept. 22, 2004).

patients. The vendor originally responsible for developing the survey had outsourced this task to another vendor, which in turn developed the survey in such a way that allowed patients to view other patients' medical information. Similarly, in 2003, a downstream vendor located outside of the United States threatened to disclose personal health information in an attempt to secure payment for her transcription services. Before this incident, officials at the U.S. medical center responsible for the patients' information were not aware of the full extent to which their local medical transcription company had subsequently outsourced its services to other vendors.

This report focuses on privacy issues associated with outsourcing services involving the use of personal health information in the administration of Medicare, Medicaid, and TRICARE. Specifically, we (1) examined the extent to which the Medicare and TRICARE federal contractors and state Medicaid agencies outsource—domestically or offshore—services involving the use of personal health information; (2) identified measures recommended by privacy experts for safeguarding outsourced personal information and examined use of these measures by the federal contractors and state Medicaid agencies; and (3) determined whether the federal contractors and state Medicaid agencies have experienced privacy breaches and whether the federal agencies that oversee Medicare, Medicaid, and TRICARE require notice from them when privacy breaches occur. We prepared this report under the Comptroller General's authority to conduct evaluations on his own initiative.[3]

To address these issues, we surveyed federal Medicare and TRICARE contractors and all state Medicaid agencies—a combined total of 378 entities—asking them to provide information on the extent to which they outsourced services involving personal health information, domestically and offshore, in 2005. We sent our survey to all Medicare Advantage contractors (252) and Medicare fee-for-service (FFS) contractors (59),[4] the 11 national level TRICARE contractors, and all 56 state Medicaid agencies. We received survey responses from 80 percent of state Medicaid agencies, 69 percent of Medicare Advantage contractors, 76 percent of Medicare

[3]See 31 U.S.C. § 717(b)(1)(2000).

[4]In the traditional Medicare program, which we call Medicare FFS, participating providers bill Medicare to receive payment for health care services provided to beneficiaries. In the Medicare Advantage program, participating health plans receive a monthly set payment amount for each enrolled beneficiary for all Medicare-covered services provided.

FFS contractors, and 73 percent of TRICARE contractors. Because the Medicare Part D outpatient prescription drug benefit began after we initiated our survey, matters related to the administration of this benefit were outside the scope of our work.

Because some firms hold more than one contract, we asked the firms to complete a separate survey for each of their contracts with the federal agencies.[5] Consequently, for analysis and reporting purposes, we considered each contract separately. Furthermore, to obtain information about downstream outsourcing, we asked respondents whether each of their three largest vendors further transferred personal health information, and if so, to which country.

To identify measures recommended by experts for safeguarding personal information when outsourcing, we conducted a literature review on this topic and confirmed our findings through interviews with privacy experts representing industry, regulatory, and consumer perspectives. We did not independently evaluate the feasibility, potential cost, or effectiveness of implementing the experts' recommended practices. We included questions on the use of these measures in our survey of federal contractors and state Medicaid agencies.

Through the survey, we also asked federal contractors and state Medicaid agencies to report whether they or their vendors experienced a privacy breach during the previous 2 years. In addition, to examine the extent to which the federal agencies that oversee Medicare, Medicaid, and TRICARE require notification of privacy breaches, we interviewed officials at the Department of Health and Human Services' Centers for Medicare & Medicaid Services (CMS)—the federal agency that oversees Medicare and Medicaid—and the Department of Defense's TRICARE Management Activity (TMA), which oversees TRICARE. We also examined the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule,[6] but did not assess compliance with HIPAA or other federal laws or regulations. We also reviewed information from secondary sources on

[5]For example, 42 firms held the 59 Medicare FFS contracts included in our study.

[6]The HIPAA Privacy Rule implements certain parts of the Health Insurance Portability and Accountability Act of 1996 regarding the privacy of health information. *See* Pub. L. No. 104-191, §§ 262-264, 110 Stat. 1936, 2033; 67 *Fed. Reg.* 53182 (2002). The HIPAA Security Rule implements HIPAA requirements for the security of health information. *See* 68 *Fed. Reg.* 8334 (2003).

data privacy laws in selected countries that are common destinations for offshore outsourcing.

We conducted our work from October 2004 through July 2006 in accordance with generally accepted government auditing standards. (See app. I for additional information on our scope and methodology.)

Results in Brief

Federal contractors and state Medicaid agencies widely reported domestic outsourcing of services involving the use of personal health information but little direct offshore outsourcing. Among survey respondents, more than 90 percent of Medicare contractors and state Medicaid agencies and 63 percent of TRICARE contractors reported some domestic outsourcing in 2005. Typically, survey groups reported engaging from 3 to 20 U.S. vendors. One federal contractor and one state Medicaid agency reported outsourcing services directly offshore. However, the federal contractors and state Medicaid agencies also reported that offshore outsourcing is initiated by their domestic vendors. Thirty-three Medicare Advantage contractors, 2 Medicare FFS contractors, and 1 Medicaid agency indicated that their domestic vendors transfer personal health information offshore, although they did not provide information about the scope of personal information transferred offshore. Moreover, the reported extent of offshore outsourcing may be understated because many of the federal contractors and agencies did not know whether their domestic vendors transferred personal health information to other locations or vendors. Specifically, 57 percent of Medicare Advantage contractors, 29 percent of Medicare FFS contractors, 26 percent of state Medicaid agencies, and 20 percent of TRICARE contractors reported that they did not know whether their largest domestic outsourcing vendors had further transferred personal health information.

Privacy experts have emphasized that provisions in contracts between firms and their vendors are important to ensuring privacy when outsourcing services that involve personal information. They also suggest that in addition to contracts, safeguard measures should be considered to protect privacy when outsourcing. These measures include assessing potential vendors' privacy practices when making selection decisions, monitoring vendor performance of privacy practices, and being aware of downstream outsourcing by vendors. The federal contractors and state Medicaid agencies we surveyed that outsource services involving personal health information vary in their use of these expert-recommended safeguard measures. Implementation of all of these expert-recommended measures was reported by 60 percent of TRICARE contractors, 51 percent

of Medicaid agencies, 29 percent of FFS contractors, and 27 percent of Medicare Advantage contractors.

In responding to our survey, over 40 percent of the federal contractors and state Medicaid agencies reported that they experienced a recent privacy breach involving personal health information. By survey group, 47 percent of Medicare Advantage contractors reported privacy breaches within the past 2 years, as did 44 percent of Medicaid agencies, 42 percent of Medicare FFS contractors, and 38 percent of TRICARE contractors. (The frequency or severity of breaches was not reported.) TMA and CMS differ in their requirements for notification of privacy breaches. TMA requires monthly reports on privacy breaches from its TRICARE contractors and follows up with contractors that report recurring lapses in privacy. CMS requires Medicare FFS contractors to report privacy breaches within 30 days of discovery, and to submit corrective action plans designed to prevent similar breaches. However, such oversight is lacking for privacy breaches that may occur with personal health information held by state Medicaid agencies and Medicare Advantage contractors, as CMS does not require reports of privacy breaches from these entities.

To help ensure that the personal health information entrusted to these federal and state health programs is being adequately protected and to facilitate prompt corrective action when appropriate, the privacy breach notification requirements that currently apply to TRICARE and Medicare FFS contractors should also apply to other Medicare contractors that handle personal health information (such as Medicare Advantage contractors) and to state Medicaid agencies. We recommend that the Administrator of CMS require all Medicare contractors responsible for safeguarding personal health information and state Medicaid agencies to notify CMS of the occurrence of privacy breaches.

In commenting on a draft of this report, CMS concurred with our recommendation and described recent steps the agency has taken to obtain information on privacy breaches from Medicare Advantage contractors. DOD concurred with our findings on TRICARE.

Background

Private Firms and State Agencies Help Administer Medicare, Medicaid, and TRICARE

As shown in table 1, CMS and TMA contract with numerous firms to perform many of the functions necessary to administer the Medicare and TRICARE programs. In addition, state agencies administer the Medicaid program.

Table 1: Administration of Federal and State Health Insurance Programs

Agency	Health program	Number of contracts in 2005
CMS	Medicare Advantage program	252 Medicare Advantage contracts
CMS	Medicare FFS program	59 FFS contracts
CMS and states	Medicaid program	56 state Medicaid agencies[a]
TMA	TRICARE program	11 TRICARE contracts

Sources: CMS and TMA.

[a]Includes the 50 states, the District of Columbia, Puerto Rico, and U.S. territories.

Federal contractors and state Medicaid agencies perform a wide variety of functions that require the use of personal health information. Such information may include medical diagnosis and treatment records and patient identifiers, such as name, address, date of birth, Social Security number, and evidence of insurance coverage. For example, when making a claims payment determination, federal contractors and state Medicaid agencies verify patient eligibility and assess whether the services provided were medically necessary. In some cases, assessing medical necessity requires a review of the patient's medical history and treatment records. In addition to claims processing, federal contractors and state Medicaid agencies use personal health information when enrolling beneficiaries, operating telephone call centers, conducting disease management programs, administering pharmaceutical benefit management services, and performing fraud investigations.

Laws Require Safeguards for Medicare, Medicaid, and TRICARE Personal Health Information

A number of laws provide protection for personal health information. Under the HIPAA Privacy Rule, certain health care organizations and individuals—known as covered entities—are required to ensure that patients' personal health information is not improperly disclosed.[7] Covered entities—health care providers, health plans, and health care clearinghouses—must develop policies and procedures for protecting health information.[8] These include restricting the amount of information disclosed to the minimum necessary to accomplish the intended purpose and to the workforce needing access. Other requirements under the HIPAA Privacy Rule include designating a privacy official and training employees on the covered entity's privacy policies.

Certain HIPAA Privacy Rule safeguards also apply to "downstream users"—whether or not they are covered entities—through contractual agreements. The HIPAA Privacy Rule requires covered entities to enter into "business associate agreements" with other firms or individuals to which they transfer personal health information for certain clinical, operational, or administrative functions.[9] Business associate agreements must establish the conditions under which a downstream vendor may use and disclose personal health information and the privacy safeguards they must apply. Covered entities are not required, under the rule, to monitor their business associates' use of privacy safeguards, but must take corrective action if they become aware of a pattern of activity or practice that amounts to a material breach of the agreement.

The HIPAA Privacy Rule applies directly to state Medicaid agencies, Medicare Advantage contractors, and TRICARE contractors that act as health plans or providers, and indirectly to Medicare FFS contractors and other TRICARE contractors. Specifically, state Medicaid agencies,

[7]In general, the HIPAA Privacy Rule addresses the use and disclosure of "protected health information," which includes any oral or written information related to an individual's past, present, or future physical or mental medical condition, health care treatment, or payment. *See* 45 C.F.R. § 160.103 (2005). In addition, the information must either identify an individual or be of a kind that could reasonably lead to the identification of an individual.

[8]In general, health care providers—such as hospitals, physicians, dentists, and pharmacies—that transmit health information electronically must comply with HIPAA requirements. Health plans are individual and group plans that provide or pay for the cost of medical care. Clearinghouses, in general, are entities that facilitate the flow of personal health information, usually between providers and payers, by transforming information submitted in nonstandard form into a standard electronic format.

[9]*See* 45 C.F.R. § 160.103 (2005).

Medicare Advantage, and TRICARE contractors that act either as health plans or providers are covered entities under the HIPAA Privacy Rule, while Medicare FFS contractors and the remaining TRICARE contractors are considered business associates to CMS and TRICARE, respectively, in their capacity as program contractors. Requirements under the HIPAA Privacy Rule also apply to certain downstream vendors that receive personal health information from federal contractors and state Medicaid agencies through outsourcing arrangements.

In addition to the HIPAA Privacy Rule, U.S. law includes a number of statutes that provide privacy protections, and some of them are applicable only to federal agencies and their contractors. The Privacy Act of 1974, for example, places limitations on agencies' collection, disclosure, and use of privacy information.[10] Furthermore, the Federal Information Security Management Act of 2002 generally concerns the protection of personal information in the context of securing federal agencies' information, and requires agencies to develop information security programs that include contractors.[11] Finally, the Social Security Act requires that state Medicaid agencies limit the use and disclosure of personally identifiable information to purposes directly related to administering the state's Medicaid program.[12]

Contractors and Medicaid Agencies Commonly Outsource Domestically; Some Vendors Outsource Offshore, but Full Extent of Offshoring Is Unknown

A majority of the federal contractors and state Medicaid agencies we surveyed engage domestic vendors to perform services involving personal health information, but rarely transfer personal health information directly offshore. However, offshore outsourcing is initiated by some domestic vendors, which transfer personal health information to offshore locations. The actual prevalence of offshore outsourcing by domestic vendors may be greater than reported, as many federal contractors and state Medicaid agencies did not know whether their domestic vendors further transferred personal health information.

[10]*See* Pub. L. No. 93-579, 88 Stat. 1896.

[11]*See* Pub. L. No. 107-347, 116 Stat. 2899.

[12]*See* Social Security Act § 1902(a)(7)(A).

Majority of Federal Contractors and State Medicaid Agencies Outsource Domestically but Rarely Outsource Directly Offshore

A majority of federal contractors and state Medicaid agencies use domestic vendors to perform services involving personal health information.[13] (See table 2.) At the same time, only one Medicare Advantage contractor and one state Medicaid agency reported direct offshore outsourcing of services involving personal health information.[14] No Medicare FFS contractors or TRICARE contractors reported direct offshore outsourcing.[15]

Table 2: Domestic Outsourcing of Services Involving the Use of Personal Health Information Reported by Federal Contractors and State Medicaid Agencies, 2005

Survey group	Number of respondents	Respondents reporting domestic outsourcing	
		Number	Percentage
Medicare Advantage contractors	173	168	97
Medicare FFS contractors	45	41	91
State Medicaid agencies	45	43	96
TRICARE contractors	8	5	63

Source: GAO.

When outsourcing domestically, the federal contractors and state Medicaid agencies typically rely on more than one vendor, although the extent to which this occurs varies across the three insurance programs. In our survey, Medicare Advantage contractors reported outsourcing services involving personal health information to a median of 20 domestic vendors per contractor. In contrast, TRICARE contractors and Medicaid agencies

[13]Federal contractors and state Medicaid agencies reported outsourcing a wide variety of services involving personal health information, including enrollment, claims processing, disease management, pharmaceutical benefits management, computer network support, mailing and printing, research and analysis, and customer service.

[14]In March 2006, we reported that some work is performed offshore for the majority of states in the administration of their Food Stamp, Unemployment Insurance, Child Support Enforcement, and Temporary Assistance for Needy Families programs. See GAO, *Offshoring in Six Human Services Programs: Offshoring Occurs in Most States, Primarily in Customer Service and Software Development*, GAO-06-342 (Washington, D.C.: Mar. 28, 2006).

[15]In 2005, CMS did not prohibit contractors or state Medicaid agencies—or their vendors—from transferring personal health data offshore in outsourcing activities. Agency officials told us that, in FFS contracts awarded in 2006 and thereafter, CMS will require contractors and subcontractors to obtain written approval from CMS prior to performing work outside of the United States. TRICARE officials told us that TMA regulations do not prohibit offshore outsourcing in the TRICARE program.

reported a median of 7 domestic vendors, while Medicare FFS contractors reported a median of 3 domestic vendors per contractor.[16]

Some Domestic Vendors Outsource Offshore, but Full Extent of Data Transfers Is Unknown

Although only one federal contractor and one state Medicaid agency reported transferring personal health information directly to an offshore vendor, contractors and Medicaid agencies also reported offshore outsourcing through the activities of their domestic vendors. Specifically, federal contractors and state Medicaid agencies reported that their domestic vendors further transfer personal health information either to the vendors' offshore locations or to another vendor located outside the United States through downstream outsourcing. Nineteen percent—33 of 173—of the Medicare Advantage contractors who responded to our survey reported that one or more of their largest domestic vendors transfer personal health information to a location outside of the United States. Four percent (2 of 45) of Medicare FFS contractors and 2 percent (1 of 45) of Medicaid agencies reported offshore outsourcing initiated by domestic vendors. Although each respondent indicated that these offshore transfers involved personal health information, we did not ask for detailed information about amount of data transferred. No TRICARE contractors reported offshore outsourcing by their domestic vendors.

Our survey results may underestimate the full extent of offshore outsourcing of services involving personal health information. Some federal contractors and state Medicaid agencies did not always know whether their domestic vendors engaged in further transfers of personal health information—domestically or offshore—while others indicated that they did not have mechanisms in place to obtain such information. Medicare Advantage contractors—which have more domestic vendors per contractor than other federal contractors or state agencies in our survey—were least likely to have information about whether further data transfers were occurring on behalf of their program. When asked about their three largest domestic vendors, 57 percent of Medicare Advantage contractors reported that they did not know whether these vendors further transferred

[16]There was wide variability within each group. For instance, 25 Medicare FFS contractors outsource to 3 or fewer U.S. vendors, while 4 FFS contractors reported transferring personal health data to more than 20 vendors each.

personal health information.[17] Similarly, 29 percent of Medicare FFS contractors and 26 percent of Medicaid agencies reported that they did not have this information for all three of their largest domestic vendors. (See table 3.)

Table 3: Vendors' Offshore Outsourcing of Services Involving the Use of Personal Health Information Reported by Federal Contractors and State Medicaid Agencies, 2005

Survey group	Percentage of respondents reporting offshore data transfers by vendors	Percentage of respondents reporting lack of knowledge about whether vendors further transfer data offshore[a]
Medicare Advantage contractors	19	57
Medicare FFS contractors	4	29
State Medicaid agencies	2	26
TRICARE contractors	0	20

Source: GAO.

[a]These data reflect federal contractors' and state Medicaid agencies' knowledge of downstream outsourcing by their three largest domestic vendors.

According to our survey, most instances of offshore outsourcing by vendors occur when the domestic vendor transfers personal health information to one of its own locations outside of the United States or to an affiliated entity, such as a subsidiary, located in another country. Of the 33 Medicare Advantage contractors that reported offshore outsourcing by vendors, 30 described instances that fit this pattern. For example, one Medicare Advantage contractor reported outsourcing to a Midwest vendor a contract to scan paper claims and create and store electronic records. The vendor, which has multiple domestic and several international locations, performs these services in Mexico. In another case, a Medicare Advantage contractor reported using its wholly owned subsidiary to provide claims data entry services. Rather than using employees at its U.S. location, the subsidiary transfers the personal health information to a location it has in India, where the data entry services are performed. A Medicare FFS contractor reported a similar instance in describing its

[17]We asked federal contractors and state Medicaid agencies to report on data transfers by their three largest vendors (those with the largest contracts in terms of monetary value). Thus, our survey does not include information about offshore outsourcing by smaller vendors.

vendor's offshore outsourcing. Its domestic vendor transfers personal health information to the vendor's own facility in Jamaica to process Medicare claims.

Offshore outsourcing was also reported to occur when domestic vendors transfer data to independent, third-party vendors located in other countries. According to our survey, this type of offshore outsourcing is less common than the type in which the offshore vendor is related to the domestic vendor. Three of the 33 Medicare Advantage contractors who reported vendor-initiated offshore outsourcing indicated that their domestic vendors transfer personal health information to an independent foreign vendor. For example, a Medicare Advantage contractor reported using a domestic subsidiary to provide claims data entry services. This subsidiary, in turn, engages in downstream outsourcing with an independent vendor located in India, where the data entry services for the Medicare Advantage contractor are performed. Medicare Advantage contractors were not the only respondents to report such downstream outsourcing relationships. A state Medicaid agency reported that its domestic vendor for customer services, which include handling call center operations and member enrollment, relies on an independent vendor located in India to perform these services.

Although our survey identified several countries as locations for offshore vendors, India was the predominant destination for outsourcing services that involve personal health information. Of the 33 Medicare Advantage contractors whose domestic vendors were responsible for most of the offshore outsourcing reported in our survey, 25 reported that personal health information had been transferred to workers located in India. Less common locations included Ghana and Mexico, with nine and six instances of offshore outsourcing, respectively. (See table 4.)

Table 4: Destination Countries for Offshore Outsourcing of Services Involving the Use of Personal Health Information Reported by Federal Contractors and State Medicaid Agencies, 2005

	Number of reported data transfers from domestic vendors to an offshore location		
Country	Medicare Advantage contractors	Medicare FFS contractors	State Medicaid agencies
India	25		1
Ghana	9		
Mexico	6		
Canada			2
Jamaica		2	
Bermuda	1		
Philippines	1		

Source: GAO.

Note: When reporting on offshore outsourcing, some federal contractors and state Medicaid agencies indicated that their domestic vendors transfer personal health information to multiple destinations.

Experts Emphasize Contracts, Suggest Measures to Safeguard Privacy When Outsourcing, but Use of Measures Varies

Privacy experts have emphasized that the contracts between firms and their vendors are important to ensuring privacy when outsourcing services that involve personal information. They also suggest safeguard measures that should be considered to protect privacy when outsourcing. These include measures to be taken during the vendor selection process and after personal health information has been outsourced. Federal contractors and state Medicaid agencies responding to our survey varied substantially in their reported use of these safeguard measures.

Experts Noted the Importance of Contract Provisions in Protecting Personal Health Information

Privacy experts indicated that having specific provisions in contractual agreements is key to ensuring that personal information is properly protected when transferred to a vendor. They noted that contracts should specify the vendors' responsibilities for maintaining safeguards to protect personal information, circumstances under which personal information may be disclosed, and rules for subcontracting.

In fact, the HIPAA Privacy Rule requires such contractual agreements to protect against unauthorized disclosure of personal health information by vendors that receive such information from covered entities to perform certain clinical, operational, or administrative functions. The Privacy Rule

further specifies certain contract elements, including the conditions and safeguards for uses and disclosures of personal health information. To ensure that these conditions and safeguards also apply to downstream vendors, the Privacy Rule requires a firm's or individual's business associates to agree in writing that any subcontractor to which they subsequently transfer personal health information will also contractually agree to the same set of safeguards.

At the same time, however, privacy experts point out that differences in national data privacy laws may influence the significance of a firm's contracts with its vendors.[18] Countries differ in the scope of their data privacy laws, with some offering broader data privacy protections than those available in the United States and others with essentially no legal protections for data privacy. For example, personal data transferred to a member country of the European Union (EU) would have to be handled in a manner consistent with the European Commission's Data Protection Directive, which is generally considered to require more comprehensive data protection than does the United States.[19] By contrast, India has no law that establishes protections for personal data.[20]

When a U.S. firm does business with a vendor in a country with relatively weak or narrow data privacy protections, experts noted that the contract between the outsourcing firm and the vendor can be used to help ensure data privacy. In the United States, vendors could be held liable according to the terms of their contract with the covered entity, which they are required to have by the HIPAA Privacy Rule. To make certain that data are similarly protected when outsourcing to a country with weaker privacy protections, experts indicate that the contract should be used to specify, in

[18]For a discussion of the potential policy implications of services offshoring, see GAO, *Offshoring of Services: An Overview of the Issues*, GAO-06-5 (Washington D.C.: Nov. 28, 2005).

[19]See Commission Directive 95/46, 1995 O.J. (L 281), 31. The directive is not law in itself, but rather requires EU nations to enact their own laws to implement the directive's principles. The directive requires that data be collected only for specific and legitimate purposes, data processors must ensure that data are accurate and up to date, and the consent of the data subject is generally required for data to be processed. Finally, the directive forbids the transfer of data to countries that are not members of the EU, unless a country "ensures an adequate level of protection" for personal information.

[20]India's *Information Technology Act of 2000* sets up criminal penalties for certain breaches of confidentiality and privacy, but these privacy standards do not apply to businesses or commercial enterprises, nor does the law include a general data protection provision. See *World Data Protection Report*, April 2004, at 19.

detail, the vendor's privacy practices and the right to terminate the contract in the event of a privacy breach. The contract also may specify which country's laws will be applied to resolve disputes that arise under the contract, which has implications for both interpretation and enforcement of the contract.[21]

When considering the implications of foreign privacy laws on data transferred offshore, another factor to consider is the legal status of the vendor. The experts we consulted generally agreed that transferring personal data to an entity with an offshore location may afford—at least in theory—the same level of privacy protections available in the United States, if the offshore entity is subject to U.S. law, such as may be the case with entities with offshore locations that are incorporated in the United States.

Expert-Recommended Safeguard Measures Address Vendor Selection and Oversight

For firms seeking data protections beyond those afforded by contracts, experts recommend several safeguard measures. Specifically, experts suggest that firms transferring personal health information to vendors should assess potential vendors' privacy practices when selecting a vendor, monitor vendor performance on privacy practices, and be aware of downstream outsourcing.

Assess Potential Vendors' Privacy Practices When Selecting a Vendor

Experts recommended that in the vendor selection process, firms assess potential vendors' privacy practices.[22] In addition to evaluating a vendor's written policies, experts suggested that the overall importance afforded privacy within the organization's culture may be an equally significant factor, as it drives the likely implementation of written privacy policies.

Experts noted different approaches to evaluating potential vendors. Describing his organization's informal approach, the privacy officer for a large provider group explained that he consults with other clients of the vendor about their level of satisfaction and considers the vendor's long-term stability and reputation. In contrast, the chief privacy officer for a

[21]Contractual agreements generally include a "choice of law" provision that specifies which jurisdiction's laws would apply in addressing a dispute over privacy issues.

[22]See Michael Rasmussen and Stephanie Moore, *Best Practices: Managing Information Risk in Business Partner Relationships*, (Forrester Research, Inc., Sept. 7, 2004). Also, R. DeLotto, *Research Note: Some U.S. Outsourcing Risks Are Often Overlooked* (Gartner, Inc., June 17, 2003).

large information technology company described her firm's formal process for evaluating potential vendors. Using written risk-rating criteria, her firm's legal and procurement departments evaluate potential vendors' privacy practices. Beyond informing selection decisions, the criteria subsequently serve as the basis for vendor evaluation and auditing. When considering a potential vendor, some experts suggested that the extent of the assessment should be determined by the perceived data privacy risk—such as the sensitivity of the data being transferred.

Monitor Vendor Performance on Privacy Practices

Experts also emphasized the importance of ongoing oversight of vendors and their activities, noting that monitoring vendor performance on privacy practices helps to ensure that contractual agreements are implemented.[23] Experts described monitoring activities as a good risk management practice, and particularly important if the vendor is performing a critical business function or handling very sensitive personal health information.[24] As one approach, a privacy expert suggested that outsourcing firms should require regular reports from vendors describing compliance efforts, privacy violations, and the use of any downstream vendors.[25]

While privacy experts recognized monitoring as a valuable safeguard, some said that adequate monitoring may be a challenge to implement. Vendors—especially those with substantial market power—may be reluctant to allow monitoring of their operations. In other cases, outsourcing firms may find it impractical or may not have sufficient resources to monitor each of their vendors. In such a situation, experts suggested that monitoring efforts should be focused on vendors that handle the most sensitive information, handle the largest volume of personal data, or have the highest risk for privacy breaches. With respect

[23]In recommending privacy practices that should be followed by financial institutions when outsourcing, the Federal Deposit Insurance Corporation highlighted monitoring activities as a best practice. Specifically, it noted that financial institutions should implement an effective oversight program and evaluate audits and reviews of the service provider's performance. See Federal Deposit Insurance Corporation, *Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks* (June 2004).

[24]The use of monitoring and auditing is one of the seven elements of a corporate compliance program, as defined in the Federal Sentencing Guidelines for Organizations. See Health Care Compliance Association, *Evaluating and Improving A Compliance Program* (Apr. 4, 2003).

[25]See Dorthula H. Powell-Woodson, Steven Morgan, and Adam Rogers, *Should Health Plans Audit Business Associates for HIPAA Privacy Rule Compliance?* (Privacy In Focus, Wiley Rein & Fielding LLP, August 2005).

to monitoring the operations of geographically distant vendors, experts stressed that alternatives to traditional monitoring may be used to minimize logistical challenges, such as hiring a third-party audit organization to conduct regular on-site visits.

Be Aware of Further Subcontracting

Experts stressed that information about the number, and identity, of vendors that handle personal information is critical to the outsourcing firm's ability to assess and mitigate privacy risks.[26] One expert we spoke with explained that with information about its vendors' downstream data transfers, the outsourcing firm is in a better position to monitor how its data are being handled. Some outsourcing firms require their vendors to obtain approval prior to subcontracting, while others require vendors to report regularly on all subcontractors. In some cases, however, information about downstream vendors can be difficult to obtain, experts noted. One expert on corporate compliance cautioned that vendors may resist such prior approvals and reporting requirements, citing the need for flexibility in responding quickly to changes in workload.

Use of Expert-Recommended Safeguard Measures Is Uneven across Federal Contractors and State Medicaid Agencies

Federal contractors and state Medicaid agencies that outsource services involving personal health information varied substantially in their reported use of the three expert-recommended safeguard measures.[27] For example, 39 percent of Medicare FFS contractors reported taking steps to assess potential vendors' privacy practices compared with 67 percent of state Medicaid agencies. With respect to monitoring vendors' privacy practices, 42 percent of Medicare FFS contractors reported doing so compared with 100 percent of TRICARE contractors. Forty-five percent of Medicare Advantage contractors reported awareness of downstream outsourcing compared with 74 percent of Medicaid agencies. With respect to the three recommended measures together, Medicare Advantage and Medicare FFS contractors reported the lowest use rates, at 27 and 29 percent, respectively. Use of the three recommended measures was more common

[26]In its June 2004 report on privacy risks associated with offshore outsourcing by financial institutions, the Federal Deposit Insurance Corporation noted that "undisclosed third-party contracting arrangements may increase risk in outsourcing relationships." It went on to recommend that "financial institutions that outsource data to domestic vendors should be aware when domestic vendors have in turn subcontracted out that same work to overseas or domestic third parties."

[27]It was beyond the scope of this engagement to assess to what extent use of these measures represented compliance with federal laws and policies, including HIPAA, the Privacy Act, and the Federal Information Security Management Act.

among Medicaid agencies, at 51 percent, and TRICARE contractors, with 60 percent.[28] (See table 5.)

Table 5: Percentage of Federal Contractors and State Medicaid Agencies That Outsource Services Involving Personal Health Information Reporting Use of Recommended Safeguard Measures

Recommended safeguard measure	Medicare Advantage contractors (n=168)	Medicare FFS contractors (n=41)	State Medicaid agencies (n=43)	TRICARE contractors (n=5)
Assess privacy practices when selecting a vendor	44	39	67	60
Monitor vendor performance on privacy practices	49	42	72	100
Be aware of further subcontracting	45	63	74	60
Use of all three measures	27	29	51	60

Source: GAO.

Many Federal Contractors and State Medicaid Agencies Experience Privacy Breaches, but Not All Are Required to Report Breaches to Federal Agencies

Our survey results show that a substantial number of federal contractors and state Medicaid agencies reported privacy breaches involving personal health information. However, TMA and CMS—the federal agencies that oversee the TRICARE, Medicare, and Medicaid programs—differ in their requirements for notification of privacy breaches involving personal health information. TMA requires reports of privacy breaches from all of its contractors. CMS collects such information from FFS contractors but not from Medicare Advantage contractors or from state Medicaid agencies.

[28]Beyond the three measures recommended by experts, federal contractors and state Medicaid agencies reported other strategies for ensuring information privacy when outsourcing. For instance, all TRICARE contractors, and nearly all Medicare Advantage contractors, have conducted a privacy risk assessment at least once, as have 88 percent of state Medicaid agencies and 53 percent of Medicare FFS contractors.

Many Federal Contractors and State Medicaid Agencies Reported a Breach of Data Privacy

In responding to our survey, over 40 percent of federal contractors and state Medicaid agencies indicated that they, or one of their vendors, experienced a privacy breach involving personal health information in 2004 or 2005. Among Medicare Advantage contractors, 47 percent reported recent privacy breaches, as did 42 percent of Medicare FFS contractors, 44 percent of Medicaid agencies, and 38 percent of TRICARE contractors. (See table 6.) These rates are comparable to the rate recently reported by commercial health insurers. In a 2005 health care industry survey, 45 percent of commercial health insurers reported the occurrence of at least one privacy breach from January through June 2005.[29]

Table 6: Federal Contractors and State Medicaid Agencies that Reported Having a Privacy Breach in 2004 or 2005

	Respondents reporting a privacy breach	
Survey group	**Number**	**Percentage**
Medicare Advantage contractors	81	47
Medicare FFS contractors	19	42
State Medicaid agencies	18	40
TRICARE contractors	3	38

Source: GAO.

Note: Contractors and state Medicaid agencies reported whether they, or one of their vendors, had experienced a privacy breach during the 2-year period.

It is difficult to interpret these data, because we did not ask respondents for information about the frequency or severity of their privacy breaches. The reported privacy breaches could have involved inappropriate disclosure of limited personal health information, such as mailing an insurance statement to the wrong address, or extensive disclosures, such as privacy breaches that involved information on many individuals or that occurred repeatedly.[30]

[29]See HIMSS/Phoenix Health Systems, *U.S. Healthcare Industry HIPAA Compliance Survey Results: Summer 2005* (August 2005).

[30]We also did not ask to what extent any of these breaches may have resulted from a violation of existing privacy and security standards.

Federal Agencies Differ in Requirements for Notification of Privacy Breaches

The federal agencies with responsibility for these programs vary in their requirements with respect to notification of privacy breaches. Since 2004, TMA has required all TRICARE contractors to report monthly on privacy breaches, including those experienced by each vendor handling enrollees' personal health information and by health care providers. According to TRICARE officials, monthly reports provide detailed information about each privacy breach, including the contractor's assessment of the "root cause" of the breach and steps taken to prevent further occurrences. TMA officials indicated that most privacy breaches occur at the vendor level or with health care providers, rather than with TRICARE contractor staff.

During 2005, three large regional TRICARE contractors reported more than 130 separate privacy breaches to TMA officials.[31] TMA officials told us that most breaches occurred inadvertently, such as when personal information was transferred to the wrong person because of incorrect mailing addresses (electronic and paper mail) or fax errors. In other cases, breaches occurred when health care providers or contractor staff—such as call center employees—inappropriately discussed personal health information with other employees. TMA officials said that the agency analyzes trends in the monthly reports and follows up with federal contractors that report recurring lapses in privacy.

In May 2005, CMS began requiring Medicare FFS contractors—but not Medicare Advantage contractors or Medicaid agencies—to report privacy breaches.[32] CMS officials told us that in prior years, FFS contractors reported privacy breaches to CMS regional office staff responsible for contractor oversight.[33] The agency changed its approach to monitoring privacy breaches by establishing a policy for federal contractors to notify CMS central office staff directly. Under the new policy, CMS requires FFS contractors to provide written notice, within 30 days of discovery, of all known or suspected privacy breaches, including those experienced by a vendor. These federal contractors must describe the privacy breach and

[31]Data from one TRICARE contractor were incomplete.

[32]In January 2006, CMS updated reporting guidelines that require Part D plans to notify CMS quarterly of privacy breaches.

[33]Based on data from its regional offices, CMS officials told us that four FFS contractors reported a total of 10 privacy breaches during 2003 and 2004. In one instance, during 2003, over 500 physician claims were stolen from an employee's car during a time when he was working from home.

subsequent corrective action plan—including any changes to policies, procedures, or employee training.

From May through December 2005, under the new reporting requirement, CMS received eight reports of privacy breaches from four FFS contractors.[34] CMS officials noted that most breaches occurred as a result of accidental disclosure of personal information. For example, the most commonly reported incident during 2005 occurred when beneficiary health information was mailed by a FFS contractor to the wrong health care provider.

CMS does not have comparable notice requirements for privacy breaches occurring with personal health information held by Medicare Advantage contractors or state Medicaid agencies. Agency officials told us that they do not require routine reporting of privacy breaches that may occur at these federal contractors and state Medicaid agencies or their vendors. However, based on our survey results, these contractors and agencies, and their vendors, are likely to experience privacy breaches at a rate similar to FFS contractors.

Conclusion

When federal contractors and state Medicaid agencies outsource services involving personal health information, they typically engage U.S. vendors that may further transfer the personal health information they receive to downstream domestic or offshore workers. CMS and TMA officials have only recently taken steps to oversee their federal contractors' and vendors' management of sensitive health information. While reporting data transfers and data privacy breaches is now required under the TRICARE program and the Medicare fee-for-service program, CMS has yet to establish a reporting requirement for Medicare Advantage contractors and Medicaid agencies. We believe that federal contractors and state Medicaid agencies should be held accountable for how well personal health information, held by them or disclosed to their vendors, is protected.

[34]By comparison, when responding to our survey, 19 Medicare FFS contractors reported a privacy breach. The discrepancy may be due to the different time periods for reporting. Our survey asked for privacy breaches over a 2-year period, while the CMS data represent the last 8 months of 2005.

Recommendation for Executive Action

To help ensure that the personal health information entrusted to federal and state health programs is being adequately protected and to facilitate prompt corrective action when appropriate, the privacy breach notification requirements that currently apply to TRICARE and Medicare FFS contractors should also apply to other Medicare contractors that handle personal health information (such as Medicare Advantage contractors) and to state Medicaid agencies. We recommend that the Administrator of CMS require all Medicare contractors responsible for safeguarding personal health information and state Medicaid agencies to notify CMS of the occurrence of privacy breaches.

Agency Comments and Our Evaluation

We received written comments on a draft of this report from CMS and DOD. CMS agreed with our recommendation and described recent steps the agency has taken to obtain information on privacy breaches from Medicare Advantage contractors. Specifically, CMS highlighted its June 9, 2006, memo to Medicare Advantage contractors requiring them to notify agency officials of breaches involving personal health information. CMS noted that it is developing specific instructions for its regional and central office staff about how to respond to such reports of privacy breaches. CMS also indicated that the HHS Office of Inspector General will be assisting the agency in assessing the adequacy of the Medicare Advantage contractor's systems for securing personal health information. In addition, CMS stated that it sent privacy reminder notices to the FFS contractors and selected other CMS contractors that handle beneficiaries' personal health information. Although the administration of the new Medicare Part D outpatient prescription drug benefit was outside the scope of our work, CMS noted that its new requirements for reporting privacy breaches will also apply to the contractors that implement this benefit.

CMS pointed out that the Social Security Act requires that state Medicaid agencies limit the use and release of personally identifiable information to purposes directly related to administering the state's Medicaid program. We included a reference to relevant provisions of the Social Security Act in the background section of this report.

Finally, CMS indicated that it has added language to its FFS contracts that would require contractors and subcontractors to obtain written approval from CMS prior to performing work at locations outside of the United States. In further discussion, agency officials clarified that CMS will be including this contract language in future Medicare FFS contracts. Thus, the revised language will take effect over the next several years as the current Medicare FFS contracts are competed and awarded to entities

called Medicare administrative contractors (MACs). CMS noted that 4 of the 23 MAC contracts have been awarded to date; the agency plans to complete its transition to the new MAC contracts by the end of fiscal year 2009.

DOD concurred with our report findings and provided a technical comment which we incorporated.

We have reprinted the letters from CMS and DOD in appendixes II and III.

We will send copies of this report to the Administrator of CMS, the Secretary of Defense, appropriate congressional committees, and other interested parties. Copies will be made available to others upon request. The report is also available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions about matters discussed in this report, please contact me at (312) 220-7600 or at aronovitzl@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who contributed to this report are listed in appendix IV.

Leslie G. Aronovitz
Director, Health Care

List of Committees

The Honorable John Warner
Chairman
The Honorable Carl Levin
Ranking Minority Member
Committee on Armed Services
United States Senate

The Honorable Charles E. Grassley
Chairman
Committee on Finance
United States Senate

The Honorable Edward M. Kennedy
Ranking Minority Member
Committee on Health, Education, Labor, and Pensions
United States Senate

The Honorable Joseph I. Lieberman
Ranking Minority Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Gordon H. Smith
Chairman
The Honorable Herb Kohl
Ranking Minority Member
Special Committee on Aging
United States Senate

The Honorable Duncan L. Hunter
Chairman
The Honorable Ike Skelton
Ranking Minority Member
Committee on Armed Services
House of Representatives

The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

The Honorable Henry A. Waxman
Ranking Minority Member
Committee on Government Reform
House of Representatives

The Honorable Charles B. Rangel
Ranking Minority Member
Committee on Ways and Means
House of Representatives

The Honorable Sherrod Brown
Ranking Minority Member
Subcommittee on Health
Committee on Energy and Commerce
House of Representatives

The Honorable Nancy L. Johnson
Chairman
The Honorable Pete Stark
Ranking Minority Member
Subcommittee on Health
Committee on Ways and Means
House of Representatives

Appendix I: Scope and Methodology

We focused our review on Medicare, Medicaid, and the Department of Defense's TRICARE program, which together cover over 100 million Americans. In this report we (1) examined the extent to which the Medicare and TRICARE federal contractors and state Medicaid agencies outsource—domestically or offshore—services involving the use of personal health information; (2) identified measures recommended by privacy experts for safeguarding outsourced personal information and examined use of these measures by the federal contractors and state Medicaid agencies; and (3) determined whether the federal contractors and state Medicaid agencies have experienced privacy breaches and whether the federal agencies that oversee Medicare, Medicaid, and TRICARE require notice from them when privacy breaches occur.

To determine the extent of service outsourcing, use of recommended practices, and experience with privacy breaches, we surveyed the federal contractors and state Medicaid agencies responsible for performing many of the administrative tasks associated with the day-to-day operations of Medicare, Medicaid, and TRICARE. In August 2005, we sent our survey to all 56 state Medicaid agencies, 252 Medicare Advantage contractors, 59 Medicare fee-for-service (FFS) contractors, and 11 TRICARE contractors. The federal contractors included in our survey were all those that held contracts with the Department of Health and Human Services' Centers for Medicare & Medicaid Services (CMS) and the Department of Defense's TRICARE Management Activity (TMA) to participate in these programs at the national level, as of January 2005. In some cases, a firm could have more than one contract. For example, the 59 Medicare FFS contracts included in our study were held by 42 firms in January 2005. In these instances, we sent the firms a separate survey for each of their contracts with the federal agencies. Consequently, for analysis and reporting purposes, we considered each contract separately. Survey response rates ranged from 69 percent (Medicare Advantage contractors) to 80 percent (state Medicaid agencies). (See table 7.)

Table 7: Survey Response Rate by Group

Survey group	Number surveyed	Number of responses	Rate of response (percentage)
Medicare Advantage contractors	252	173	69
Medicare FFS contractors	59	45	76
State Medicaid agencies	56	45	80
TRICARE contractors	11	8	73

Source: GAO.

Survey questions addressed whether the federal contractor or state Medicaid agency outsourced services during 2005—domestically or offshore—that involved the use of personal health information. We asked the federal contractors and state Medicaid agencies that used outsourcing to provide the total number of domestic and offshore outsourcing agreements. To obtain information about downstream outsourcing, we asked respondents whether each of their three largest vendors further transferred personal health information, and if so, to which country.

For most survey items, we did not independently verify information provided by respondents. However, we performed quality checks, such as reviewing survey data for inconsistency errors and completeness. When necessary, we contacted survey respondents to obtain clarification before conducting our analyses. Our analysis of respondents and nonrespondents in each survey group, on variables such as entity size, type, and geographic location, did not identify substantial differences, suggesting that the risk of respondent bias is low. Among the survey items we reported on, we did not find substantial variation in item response rate. Based on these efforts, we determined that the survey data were sufficiently reliable for the purposes of this report.

To identify privacy practices recommended by industry experts to protect personal information from inappropriate disclosure when outsourcing, we reviewed relevant literature on privacy practices, domestic outsourcing, and offshore outsourcing. Our review included perspectives from the health care and financial business sectors, including syntheses of best practices. Using a structured interview guide, we then interviewed privacy experts to identify commonly recommended business practices for protecting the privacy of personal information when outsourcing. We selected individuals to interview based upon literature they published on the topics of outsourcing and privacy protections and through referrals

from other experts. We interviewed experts representing industry, consumer, and regulatory perspectives. We did not independently evaluate the feasibility, potential cost, or effectiveness of implementing experts' recommended practices. Survey questions asked whether federal contractors and state Medicaid agencies routinely use these expert-recommended practices. We did not review to what extent the practices used by the federal contractors and Medicaid agencies comply with existing statutory and administrative requirements.

Through the survey, we also asked the federal contractors and state Medicaid agencies to report on their experience with privacy breaches during the previous 2 years. To obtain information on federal agencies' requirements for notification of privacy breaches experienced by the federal contractors and state Medicaid agencies, we interviewed officials at TMA and CMS—the federal agency with oversight responsibility for Medicare and Medicaid. We asked agency officials to provide us with summary data on the number and type of privacy breaches reported by federal contractors and state Medicaid agencies during 2004 and 2005. We did not provide a definition of privacy breach in the survey. We also examined the Health Insurance Portability and Accountability Act and its implementing regulations, but did not assess compliance with them or with other federal laws and regulations. In addition, we reviewed information on data privacy laws in selected countries that are destinations for offshore outsourcing. We conducted our work from October 2004 through July 2006 in accordance with generally accepted government auditing standards.

Appendix II: Comments from the Centers for Medicare & Medicaid Services

DEPARTMENT OF HEALTH & HUMAN SERVICES

Centers for Medicare & Medicaid Services

Administrator
Washington, DC 20201

DATE: AUG - 4 2006

TO: Leslie G. Aronovitz
Director, Health Care
Government Accountability Office

FROM: Mark B. McClellan, M.D., PhD.
Administrator

SUBJECT: Government Accountability Office's (GAO) Draft Report, "Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid and TRICARE" (GAO-06-676)

The Centers for Medicare & Medicaid Services (CMS) has reviewed the GAO draft report entitled Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid and TRICARE. We appreciate the information, and we agree that protecting personal health information is a top priority.

We concur with the recommendation made in the report, that CMS should require all plans/contractors to notify us in any case of security breach involving personal health information. In fact, CMS has already begun taking action. We are speaking to plans about security breaches, and safeguards for personal health information. For plans with offshore vendors, we will require them to describe what they do to protect beneficiary information. The report does not take into account recent CMS actions, prior to our receipt of GAO's report. The GAO report states that it covers the time frame of November 2004 through July 2006, but it does not mention any of CMS' actions listed below.

- Medicare Part D Reporting Requirements for 2006, Section V, Grievances, (G) requires quarterly reporting of the number of confidentiality/privacy grievances received related to Part D. Examples include, but are not limited to, potential violations of medical information privacy standards by the plan or pharmacy.

- As a result of the recent violations, CMS sent a memo to all Medicare Advantage (MA) and Part D plans via Health Plan Management System (HPMS) on June 9 reminding them of the CMS requirements regarding the protection of personal health information, and requiring plans to notify CMS of any security breaches involving personal health information.

- CMS notified all associate regional administrators and branch chiefs, on July 11 that all suspected security violations involving MA and prescription drug plan (PDP) sponsors must be reported to Central Office (CO). Reporting to CO will

1

ensure CMS responds to all security incidents in a consistent manner. In addition, the regions were asked to report to CO any known security incidents/ violations involving MA and PDP sponsors that have occurred since January 2006.

- CMS is crafting specific instructions for CO and Regional Office plan and account managers, regarding what they are to do and whom they are to notify in the event that a health plan self-discloses a privacy violation. These instructions will be incorporated into the Standard Operating Procedures for Parts C & D.

- Finally, the Office of Inspector General (OIG) will be assisting CMS in investigating health plan capability in this area. The OIG held an entrance conference on Tuesday July 25 with CMS. Their scope of work includes assessing whether contracted health plans have adequate security controls in place for handling personal health information.

The following CMS components have also sent privacy reminder notices to their business partners.

Dates	From	To
July 7, 2006	Office of Financial Management	All Program Safeguard Contractors
July 11, 2006	Center for Medicare Management	Fiscal Intermediaries, Carriers and Durable Medical Equipment Regional Carriers
July 11, 2006	Center for Medicare Management	Durable Medical Equipment Medicare Administrative Contractors
July 11, 2006	Office of Information Services	Shared System Maintainers & Data Centers
July 12, 2006	Office of Research, Development & Information	Researchers and Demonstration Plans

The Center for Medicaid and State Operations is preparing a policy statement to State Medicaid Directors concerning data privacy and security.

The report fails to note that State Medicaid agencies are governed primarily by section 1902(a)(7) of the Social Security Act rather than the Health Insurance Portability & Accountability Act of 1996 (HIPAA) with respect to confidentiality of personally identifiable information about applicants or recipients. The HIPAA provides that it does not preempt more restrictive Federal or State laws regarding confidentiality of personally identifiable information. Section 1902(a)(7) is a much more restrictive provision. Under section 1902(a)(7) the use or release of personally identifiable information is prohibited unless for a purpose directly connected to administration of the plan. Federal regulations further provide that the Medicaid agency must restrict access to information about applicants or recipients to "persons or agency representatives who are subject to standards of confidentiality that are comparable to those of the agency" (42 CFR 431.306(b)). Thus, any contract between a Medicaid agency and a fiscal agent or other

contractor must restrict the use or release of personally identifiable information to the purposes directly connected with administration of the plan as defined by Federal regulations at 42 CFR 431.302. Any sub-contractor of the State's prime contractor must also be bound by the same rules.

Although CMS does not have regulations that require MA and Part D plans to report to CMS the disclosure of personally identifiable information, CMS does have regulations (at 42 CFR 422.80) that require approval of marketing materials. Federal regulations at 42 CFR 422.80 require that CMS approve marketing materials prior to distribution. The notification letters to beneficiaries for these privacy violations fall under the definition of marketing materials. Since the beneficiary letters must be approved prior to distribution, the MA organization would have to notify CMS of the privacy disclosure in order to receive approval on the beneficiary notification letter. As a result, CMS must be notified of any disclosure of this type.

Our review indicates that while MA and Part D organizations are obligated to adhere to the HIPAA administrative simplification rules, HIPAA does not require them to self-report confirmed or suspected HIPAA violations to CMS. A review of our disclosure requirements further clarifies that CMS does not require specific self-reporting of suspected HIPAA violations to CMS.

- The Center for Medicare Management within CMS has included language in its contracts that specifies the criteria an offshore contractor must meet. The Center for Beneficiary Choices is looking to replicate this action for 2008. The Center for Medicare Management contract requirement is as follows:

H. 22- WORK PERFORMED OUTSIDE THE UNITED STATES AND ITS TERRITORIES

The contractor, and its subcontractors, shall not perform any activities under this contract at a location outside the United States without the prior written approval of the Contracting Officer. In making a decision to authorize work outside the United States, the Contracting Officer will consider the following factors, including but not limited to:

1) All contract terms regarding systems security
2) All contract terms regarding the confidentiality and privacy requirements for information and data protection
3) All contract terms that are otherwise relevant, including the provisions of the statement of work
4) Corporate compliance
5) All laws and regulations applicable to the performance of work outside the United States
6) The best interests of the United States

In order to secure the Contracting Officer's authorization to perform work outside the United States, the contractor must demonstrate that the performance of work outside the United States satisfies all of the above factors. If, in the Contracting

Officer's judgment, the above factors are not fully satisfied, the performance of work outside the United States will not be authorized.

We appreciate the efforts of the GAO, and reassert our commitment to protecting beneficiary health information. We believe our actions thus far demonstrate our ability to work with our contractors to that end, and we will continue to require strict protection of personal health information. We look forward to working with the GAO as we proceed to address this issue, for the well-being of all Medicare and Medicaid beneficiaries.

Appendix III: Comments from the Department of Defense

THE ASSISTANT SECRETARY OF DEFENSE

1200 DEFENSE PENTAGON
WASHINGTON, DC 20301-1200

HEALTH AFFAIRS

JUL 18 2006

Ms. Leslie G. Aronovitz
Director, Health Care
United States Government Accountability Office
Washington, DC 20548

Dear Ms. Aronovitz:

This is the Department of Defense (DoD) response to the Government Accountability Office (GAO) draft report: "PRIVACY: Domestic and Offshore Outsourcing of Personal Information in Medicare, Medicaid and TRICARE," dated July 7, 2006 (GAO Code 290393/GAO-06-676).

Thank you for the opportunity to review and comment on the draft report. Overall, we concur with the report findings. However, it was determined that one paragraph was in error and DoD recommends this paragraph be updated per the suggestion in the enclosure.

Our specific comments on the GAO draft report, its findings, and the recommendations are attached in the enclosure.

Again, thank you for the opportunity to provide these comments. My points of contact for additional information are Mr. Sam Jenkins (functional) at (703) 681-6077 or Mr. Gunther J. Zimmerman (Audit Liaison) at (703) 681-3492.

Sincerely,

William Winkenwerder, Jr., MD

Enclosure:
As stated

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Leslie G. Aronovitz, (312) 220-7600 or aronovitzl@gao.gov

Acknowledgments

In addition to the contact named above, Rosamond Katz, Assistant Director; Manuel Buentello; Adrienne Griffin; Jenny Grover; Kevin Milne; and Daniel Ries made key contributions to this report.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

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

Order by Mail or Phone

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

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

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

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

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

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548