United States General Accounting Office

GAO

Report to the Chairman, Subcommittee on Health, Committee on Ways and Means, House of Representatives

July 1999

MEDICARE

Improvements Needed to Enhance Protection of Confidential Health Information

GAO/HEHS-99-140

GAO

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

Health, Education, and
Human Services Division

B-282540

July 20, 1999

The Honorable Bill Thomas
Chairman, Subcommittee on Health
Committee on Ways and Means
House of Representatives

Dear Mr. Chairman:

The Health Care Financing Administration (HCFA) in the Department of Health and Human Services (HHS) processes the nation's largest collection of health care data, with information on 39 million Medicare beneficiaries. To discharge its responsibilities, HCFA must collect personally identifiable health information on Medicare beneficiaries. Such information includes names, addresses, and health insurance claim numbers as well as various diagnoses and types of treatment received by beneficiaries. This information is used by HCFA for a variety of purposes, including the payment of approximately 900 million Medicare claims annually and the conduct of research to evaluate policy, adjust payment rates, improve program operations, improve health care quality, and make recommendations for legislative changes to the Medicare program.

The personally identifiable information that HCFA collects on Medicare beneficiaries is protected by the Privacy Act of 1974. This law, which governs the collection, maintenance, and disclosure of federal agency records, balances the government's need to maintain information about individuals with their right to be protected against unwarranted invasions of their privacy. State laws also protect the privacy of certain personally identifiable medical information, but these laws vary significantly in their scope and the specific protections they afford. To create a more uniform set of protections that would affect all users of confidential medical information, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that, unless the Congress enacts a health privacy law establishing standards for the electronic exchange of health information by August 21, 1999, HHS must promulgate such standards by regulation within the following 6 months.

In response to your request, we are reporting on four areas related to HCFA's use of personally identifiable health information: (1) HCFA's need for personally identifiable health information to manage the Medicare program and accomplish other purposes; (2) HCFA's policies and practices regarding disclosure of information on Medicare beneficiaries; (3) the

adequacy of HCFA's safeguards for protecting the confidentiality of electronic information and HCFA's monitoring of others' protection of beneficiary information; and (4) the effect on HCFA of state restrictions on the disclosure of confidential health information. Appendix I contains a discussion of our scope and methodology. We conducted our work from April through June 1999 in accordance with generally accepted government auditing standards.

Results in Brief

To carry out its legislated responsibilities, HCFA needs to collect and maintain personally identifiable health information on its 39 million Medicare beneficiaries. For example, it needs personally identifiable information about beneficiaries' demographics, enrollment, and utilization of health care services to pay claims; determine the initial and ongoing eligibility of beneficiaries; and review the care beneficiaries receive in terms of access, appropriateness, and quality. HCFA also uses this information in essential research activities that can lead to improvements in rate-setting, services provided, and quality of care.

HCFA's policies and practices regarding disclosure of personally identifiable health information are generally consistent with the provisions of the Privacy Act. For example, HCFA may disclose information without an individual's consent under certain circumstances, such as for research purposes or authorized civil and criminal law enforcement activities. In accordance with the Privacy Act, when determining whether to disclose information, HCFA officials attempt to balance the information needs of data requestors with the need to protect the confidentiality of personally identifiable health information. HCFA screens requests for personally identifiable information on Medicare beneficiaries from non-HCFA researchers more thoroughly than requests from HCFA staff who need the data to conduct the agency's business. For example, non-HCFA researchers, such as those funded by private foundations, must agree to a set of conditions specifying how they will use the data and protect beneficiaries' confidentiality, as well as provide details on how the disclosure of information will address the goals of HCFA's research program. However, we found that HCFA cannot readily provide beneficiaries with an accounting of the disclosures it makes, a capability called for by the Privacy Act. Moreover, HCFA has not adequately provided oversight agencies such as the Office of Management and Budget (OMB) with complete information on its Privacy Act activities. In addition, HCFA does not always clearly inform Medicare beneficiaries of the purposes for which their information may be disclosed to other organizations, as

required by the Privacy Act. To address these issues, HCFA has established a new executive Beneficiary Confidentiality Board and initiated a number of actions in response to January 1999 OMB guidance to all agencies to review information practices for compliance with the Privacy Act.

Although few complaints about Privacy Act violations have been made to date, weaknesses in the implementation of HCFA's policies could potentially compromise the confidentiality of health information on Medicare beneficiaries. Specifically, HHS' Office of the Inspector General (OIG) continues to find vulnerabilities in HCFA's and its contractors' management of electronic information that could lead to unauthorized individuals reading, disclosing, or tampering with confidential information. In addition, because HCFA does not routinely monitor contractors and others, such as researchers, who use personally identifiable Medicare information, its ability to prevent unauthorized disclosures or uses and to provide timely corrective action for those that might occur is not assured. HCFA officials told us they are in the process of addressing the OIG's findings. However, its ability to make progress in this area is currently affected by the agency's efforts to direct resources to address computer requirements for the Year 2000 so that there will be no interruption of services and claims payments for beneficiaries and providers.

Some states prohibit the disclosure of sensitive health-related information, such as human immunodeficiency virus (HIV) status, except for specified purposes. HCFA officials said that HCFA's policy is to respect state laws regarding sensitive health information that are more restrictive than federal requirements, so HCFA has allowed states to withhold information on HIV, acquired immunodeficiency syndrome (AIDS), and sexually transmitted diseases (STD) for certain surveys of nursing home patients. HCFA officials told us that these state laws have not prevented the agency from receiving information necessary for paying claims. However, HCFA may change its policy of allowing states to withhold this information as the agency develops and implements payment systems that depend on diagnostic information. If HCFA were restricted from receiving uniform health information from across the country, its ability to set rates, monitor quality, and conduct or support health-related research could be adversely affected.

This report makes recommendations to HCFA to improve the protection of confidential information on Medicare beneficiaries.

Background

The Medicare program, created by the Social Security Amendments of 1965 and administered by HCFA, was initially established to provide health insurance for most persons aged 65 or older. In 1972, the program was broadened to cover the disabled and patients with end-stage renal disease (ESRD) who require dialysis or kidney transplants. Medicare consists of two programs, each with its own enrollment, coverage, and financing—Hospital Insurance (commonly referred to as Part A) and Supplemental Medical Insurance (commonly referred to as Part B). Medicare Part A helps pay for hospital care, hospice care, and post-hospital care in skilled nursing facilities and by home health agencies. Medicare Part B helps pay for doctors, outpatient hospital care, home health care not covered under Part A, and other medical services such as the services of physical and occupational therapists. In addition, the Balanced Budget Act of 1997 created a new Part C, establishing Medicare+Choice which includes expansion of health plan options.

In protecting the confidentiality of health information of its beneficiaries, HCFA's activities, like those of other federal agencies, are governed by the Privacy Act of 1974. The Privacy Act requires that agencies limit their maintenance of individually identifiable records to those that are relevant and necessary to accomplish an agency's purpose. Federal agencies store personally identifiable information in systems of records. A system of records is a group of records, under the control of a federal agency, from which information can be retrieved by the name of an individual or an identifier such as a number assigned to the individual. The Privacy Act defines a record as any item, collection, or grouping of information maintained by an agency that contains an individual's name or other identifying information; for example, it could include information on education, financial transactions, and medical history. Under the Privacy Act, federal agencies must inform the public through publication in the Federal Register of any establishment or revision of a system of records. In the case of HCFA, 62 of its 81 systems of records relate directly to Medicare beneficiaries.[1] HCFA's systems of records contain information stored in electronic and paper form. HCFA stores personally identifiable data on a Medicare beneficiary's enrollment and entitlement to benefits; demographic information such as age, race, ethnicity, and language preference; and diagnoses and utilization of medical services.

The Privacy Act generally prohibits the disclosure of individuals' records without their consent. However, it allows the disclosure of information

[1]Its other systems of records contain information on Medicaid recipients, health care providers, and HCFA employees.

without an individual's consent under 12 circumstances called conditions of disclosure, such as disclosure by a federal agency to its employees based on their need for records to perform their duties. Another condition of disclosure allows an agency to establish routine uses. These are uses of the information determined by the agency to be compatible with the purposes for which it is collected and which are published in the Federal Register. Personally identifiable information can be disclosed when the agency determines that the disclosure is for an established routine use. While the Privacy Act permits agencies to disclose information, it does not require that they do so; they can, for example, determine that in a particular case the privacy interest outweighs the public interest in disclosure. However, an agency must always disclose information maintained about an individual to that individual at his or her request.

A beneficiary may bring a civil action against HCFA for alleged Privacy Act violations. These violations may include failure to grant an individual access to his or her record, amend a record as requested, or properly maintain an individual's record with adverse consequences resulting for the individual. Respective remedies include granting access to the record, amending the record, and awarding a minimum of $1,000 in damages. In all cases, successful plaintiffs also can be awarded attorney fees and litigation costs.

Criminal penalties up to $5,000 may be assessed against an agency official or employee who willfully discloses material to an agency or individual not entitled to receive it, or willfully maintains a system of records without meeting the notice requirements of the Act. Such penalties may also be assessed against anyone who knowingly and willfully requests or obtains agency records about an individual under false pretenses.

HCFA Needs Personally Identifiable Information on Medicare Beneficiaries

For HCFA, personally identifiable health information is essential to the day-to-day administration of the Medicare program. Of most significance, HCFA and its contractors need to use personally identifiable information on patients and their diagnoses and treatments to pay approximately 900 million fee-for-service claims annually from providers, suppliers, and others. HCFA also uses personally identifiable information to determine the initial and ongoing eligibility of Medicare beneficiaries, determine risk-adjusted payments, make monthly payments to more than 390 Medicare managed care plans, and track which managed care plans have been selected by over 6 million Medicare beneficiaries.

HCFA and its contractors also use data containing personally identifiable information to carry out essential program integrity activities by profiling patients and providers to identify inappropriate claims and inappropriate use of services, to prevent fraud and abuse, and to carry out investigations, as well as for other purposes. Other HCFA activities that rely on personally identifiable information include coordinating with insurers, employers, and others in administering the Medicare Secondary Payer program;[2] developing fee schedules and payment rates used in fee-for-service claims processing; reviewing the access to, appropriateness of, and quality of care received by beneficiaries; and conducting research and demonstrations including the development and implementation of new health care payment approaches and financing policies, and evaluating the effect of HCFA's programs on beneficiaries' health status.

An example of how HCFA uses personally identifiable information to improve the health of Medicare beneficiaries is the agency's ongoing campaign to increase influenza vaccination rates. Using individual identifiers, HCFA links the bills it receives to its eligibility files to determine age, gender, race, and geographic location of beneficiaries who have not received influenza vaccinations. HCFA then works with community groups to reach out to the specific groups and areas with low immunization rates. HCFA staff told us that this outreach is helping the agency make progress on meeting the Healthy People 2000 goals for immunization set by HHS.

HCFA Discloses Information About Medicare Beneficiaries for Authorized Purposes

When screening requests for identifiable information, HCFA determines whether disclosure is authorized by the Privacy Act. It also uses different levels of review depending upon the type of organization making a request for information. HCFA's policy and practice generally are to limit disclosures to information needed to accomplish the requestor's purposes. However, we have found weaknesses in its recordkeeping system for tracking and reporting on disclosures and its notices to beneficiaries that their information could be disclosed.

HCFA Screens Requests for Personally Identifiable Information

In making decisions about whether to disclose information, HCFA's primary criterion is whether the disclosure is permitted under one of the 12 conditions of disclosure in the Privacy Act. HCFA officials view the

[2]The Medicare Secondary Payer provision limits payment under Medicare if that payment has been made or can reasonably be expected to be made from another source such as under a workmen's compensation law, automobile or liability insurance policy, or certain health plans. In such cases, Medicare payments for items or services are conditional payments, and Medicare is entitled to reimbursement from the other sources for the full amount of Medicare payments.

establishment of routine uses for each of its systems of records as a key protection of personally identifiable information that could be disclosed to federal agencies other than HHS or organizations outside of the federal government. In screening requests for personally identifiable information on beneficiaries, HCFA officials attempt to balance the information needs of data requestors with the need to protect the confidentiality of beneficiaries' health information. HCFA can disclose information to publicly and privately funded researchers and to public agencies such as the Agency for Health Care Policy and Research and the Department of Veterans Affairs for health services research projects; to qualified state agencies for the purposes of determining, evaluating, or assessing cost, effectiveness, or quality of health care services provided in a state; to insurers, underwriters, employers who self-insure, and others for coordination of benefits with the Medicare Secondary Payer program; to the Bureau of the Census for census-taking purposes such as assuring an accurate count of the aged; and to congressional offices acting on behalf of beneficiaries.[3]

HCFA has different levels of review, depending upon the type of organization making a request for information. According to HCFA policy, HCFA employees and claims administration contractors are provided access to personally identifiable information on Medicare beneficiaries only when the use of such information is integral to the completion of their official duties. The decision to permit access by HCFA staff is made by officials throughout the agency who are responsible for various information systems.

HCFA places additional requirements on other HHS employees and contractors.[4] They must submit written requests and signed data use agreements to HCFA's Office of Information Services indicating their understanding of the confidentiality requirements of the Privacy Act and HCFA's data release policies and procedures. These policies and procedures include a requirement that the data user will not publish or release information that could permit deduction of a beneficiary's identity.

Other federal agencies and nonfederal organizations, such as law enforcement agencies and state governments, that seek information on Medicare beneficiaries must meet another level of requirements. HCFA staff

[3]GAO also receives personally identifiable information from HCFA. GAO's right to receive such information from federal agencies is not restricted by the Privacy Act. Federal law requires GAO to maintain the same level of confidentiality for this information as is required of the source agency.

[4]Although HHS' OIG does not follow all HCFA disclosure policies, it abides by the Privacy Act and has voluntarily signed a data use agreement with HCFA.

in the Office of Information Services first determine whether the request appears to fall within a routine use for that system of records or other condition of disclosure as allowed by the Privacy Act. If so, they determine whether the use is compatible with the purpose for which the information was originally collected or is otherwise authorized. They also review the request to ensure that all Privacy Act requirements and HCFA's data release policies are met. HCFA officials told us that they rely on the requesting organization to provide the initial certification that its activities require the personally identifiable information it is seeking. HCFA requires that the organization submit a request on its letterhead providing the purpose for which the data are needed, a description of the methodology or the project in which the data will be used, the specific files being requested, the criteria for data selections or searches, and a signed data use agreement.[5] For civil or criminal law enforcement activities, HCFA requires a written request from the head of the law enforcement agency or delegated official which references the law to be enforced and the civil or criminal court case number. When information is requested pursuant to a court order, HCFA requires a copy of the court order and guidance from HCFA's Office of General Counsel.

In screening requests for outside research projects, HCFA imposes yet another level of requirements. When research requests are received from researchers not funded by an HHS agency, HCFA officials told us that they not only conduct a review to determine whether disclosure would be permitted under the Privacy Act, but they also evaluate the requests to determine if the purpose (1) requires the use of identifiable data, (2) is of sufficient importance to warrant the risk to the individual that additional exposure of the record might bring, and (3) is likely to be accomplished because the project is soundly designed and properly financed. HCFA officials review a detailed protocol or study design to evaluate whether the proposed research will address the goals of HCFA's own research program and thus further knowledge of health care access, cost, quality, service delivery, or financing. In the case of research funded by other HHS agencies, HCFA requires, but does not itself review, a copy of the study protocol approved by project officers in agencies such as the National Institutes of Health and the Agency for Health Care Policy and Research.

Approval by the HCFA Administrator is required when researchers request the names and addresses of Medicare beneficiaries from whom they wish to collect new data. If the project is approved, the researcher must send

[5]In the case of some organizations, such as the Medicare Payment Advisory Commission and GAO, a data use agreement is requested, but not required.

potential participants a special notification letter, signed by the HCFA Administrator, indicating that HCFA is cooperating with the researcher by providing a list of potential participants for the study. The letter indicates that the beneficiaries are not required to participate in the research project and that their Medicare benefits will not be affected by their decision. Seven to 10 days after the HCFA letter is mailed, the researcher can contact the beneficiaries directly to see if they wish to participate. In a recent example, the HCFA Administrator approved a request from a university researcher for a names and addresses file of Medicare beneficiaries in two Pennsylvania cities for a study entitled, "Keeping Older Community Members Safe in Their Homes." This study, funded by the state of Pennsylvania, consists of surveys and in-home interviews and is being conducted to improve the in-home health and safety of the Medicare beneficiary population by developing community action programs in the two cities.

HCFA Generally Limits Disclosures to Information Needed to Accomplish Purposes

HCFA officials told us their practice is to disclose the least amount of personally identifiable information that will accomplish the requestor's purpose. HCFA generally provides one of three types of data files: public-use files, which are stripped of identifying information on beneficiaries; beneficiary-encrypted files, in which information is encoded or redacted; and files which contain explicitly identifiable information, such as health insurance claim numbers.[6] HCFA officials told us that they direct requestors whenever possible to either public-use files or to beneficiary-encrypted files rather than to the files containing more identifiable beneficiary information. HCFA does not generally customize data files by removing elements for the specific purpose of reducing the amount of personally identifiable information disclosed. HCFA officials told us that removing elements is resource-intensive, but they are developing software that would permit them to easily customize by data element.

Public-use files include some of the most frequently requested HCFA data used for analyzing health care spending trends and formulating programs to improve the quality and effectiveness of health care. Data elements that can directly identify an individual and elements or combinations of elements from which an individual's identity can be deduced have been removed from or summarized in these files. For example, date of birth may be converted to an element containing 5-year age groups.

[6]A health insurance claim number consists of the Social Security number of the primary Medicare subscriber followed by a letter indicating whether the number belongs to the primary holder or the spouse, as well as certain other information such as whether the beneficiary qualifies because of age or disability.

HCFA staff said that beneficiary-encrypted files may meet requestors' needs when public-use files are not adequate. In beneficiary-encrypted files, HCFA has encoded or removed the health insurance claim number, date of service, beneficiary name, beneficiary zip code, provider information, or other such elements. For example, a beneficiary's health insurance claim number would be redacted or encrypted. HCFA defines these files as "implicitly" identifiable because they contain data elements that could be combined or linked with other available information to deduce a beneficiary's identity.

Requestors may make a case to HCFA that they need files with explicitly identifiable information such as names, addresses, or health insurance claim numbers. As mentioned previously, HCFA officials have approved the disclosure of files with the names and addresses of Medicare beneficiaries. HCFA has provided researchers with data files containing health insurance claim numbers. For example, HCFA recently approved research requests for data from the Surveillance, Epidemiology, and End Results joint project conducted by HCFA and the National Cancer Institute, the ESRD file on patients receiving treatment for renal disease, and a variety of standard analytical files describing inpatient and other types of care received by Medicare beneficiaries.

Before HCFA discloses implicitly or explicitly identifiable information to other organizations, it generally requires the requestors to sign a data use agreement. By signing, a requestor agrees to abide by HCFA's confidentiality requirements including safeguarding the data, prohibiting subsequent use of the data for a different purpose, and destroying or returning the data within a specified time period. For implicitly identifiable data (beneficiary-encrypted files), requestors also must agree that they will not attempt to identify any specific individual whose record is included in the file. Recipients of public-use files are not required to sign data use agreements because these files do not contain personally identifiable health information.

HCFA's Recordkeeping System for Tracking and Reporting Has Weaknesses

HCFA is unable to readily fulfill the Privacy Act's requirement to provide beneficiaries with an accounting of the disclosures made of their personally identifiable information. In addition, the agency is unable to give oversight agencies information on related Privacy Act activities. HCFA's establishment of an executive-level beneficiary confidentiality board in May 1999 and actions it is taking in response to January 1999 guidance from OMB may help address these issues.

Although Medicare beneficiaries have the right under the Privacy Act to ask for and receive an accounting of disclosures of their personally identifiable information and to examine or amend their individual records, HCFA's recordkeeping system is incapable of readily providing an accounting of disclosures to beneficiaries. The Privacy Act requires that this accounting include information on the nature and purpose of the disclosure and the name and address of the person or organization to whom the disclosure was made. HCFA staff told us that the agency's computerized system for tracking disclosures cannot easily generate information for an individual beneficiary on disclosures made from HCFA's systems of records. HCFA's primary method of accounting for disclosures involves tracking data use agreements, which are filed by the names of requestors and not by HCFA's systems of records. However, HCFA officials told us that they were not aware of requests from any beneficiaries for information about disclosures involving their personally identifiable information.

In addition, HCFA officials told us that they are developing a system that will more easily meet current OMB requirements and better account for disclosures of personally identifiable information made to other organizations. HCFA officials told us that, as directed by OMB, they have begun reviewing their recordkeeping of activities involving the Privacy Act. As a result of a May 14, 1998, presidential memorandum directing each agency to review its information practices to ensure compliance with the Privacy Act, OMB issued guidance in January 1999 stating that agencies can protect privacy by limiting the amount of information they maintain about individuals and ensuring that such information is relevant and necessary to accomplish an agency purpose. OMB has asked agencies to reevaluate the relevance and necessity of maintaining personally identifiable information on individuals, the appropriateness of current safeguards, and the continuing justification to disclose personally identifiable information for routine uses. OMB has also asked agencies to review their procedures for accounting for disclosures to improve individuals' ability to determine who has seen their records, and when. HCFA has begun to address OMB's guidance and officials told us they are reviewing routine uses permissible for HCFA's systems of records.

In May 1999, HCFA also established a Beneficiary Confidentiality Board to review issues relating to the protection of confidential information, including HCFA's policies and procedures for disclosing personally identifiable information. The Board will consist of selected members from HCFA's executive council and will review strategic issues relating to the

protection of confidential patient information. It will focus on balancing the privacy interests of Medicare beneficiaries with the public interest of HCFA's need to collect and release individually identifiable information.

Weaknesses in HCFA's recordkeeping system also affect its ability to report on its Privacy Act activities. The Privacy Act requires the President to make a biennial report to the Congress on the Privacy Act activities of the executive branch. To implement this provision of the Privacy Act, OMB requires executive branch agencies to report the number of individuals who have requested access to their files or have requested that the agency amend the information maintained in their files. However, HCFA officials told us they did not give HHS adequate information about Medicare beneficiaries for eventual submission to OMB. As a result of our discussions with them, HCFA officials have begun to revamp their information system to more effectively report on their Privacy Act activities in 2000, when the next biennial report is due.

Notifications to Beneficiaries That Their Information Could Be Disclosed Are Not Always Clear or Comprehensive

The Privacy Act requires federal agencies to permit individuals to determine what records pertaining to them are collected, maintained, used, or disseminated by federal agencies. The Privacy Act requires an agency to notify individuals of the following when it collects information: (1) the authority under which the agency is collecting the information, (2) the principal purpose for which the information is intended to be used, (3) routine uses that may be made of the information, and (4) whether the individual is required to supply the information and the effects on the individual of not providing it.[7] Although we found that some of HCFA's Privacy Act notifications provide beneficiaries with all the information required by the Privacy Act, we found others to be deficient.

HCFA officials told us they use more than a dozen different Privacy Act notifications when collecting information from beneficiaries. Individuals are first exposed to a Medicare-related Privacy Act notice when they apply for Social Security retirement benefits and receive a multi-page Privacy Act notice. At age 65, approved Social Security retirement benefit applicants are automatically enrolled in Medicare and should receive other Privacy Act notifications whenever the agency collects information about them—such as when they separately enroll in Medicare Part B, receive medical care, participate in a survey, or enroll in a demonstration testing a new delivery or payment system. Health care providers must obtain and

[7]The Privacy Act also requires a federal agency to permit individuals to gain access to information pertaining to them in the agency's records, to have a copy made of the record, and to seek correction or amendment of the record.

keep on file beneficiaries' signatures attesting that they have been advised of the collection and use of their information. In the case of physician services, this is usually done the first time the beneficiary sees the physician. In the case of other services, such as a hospitalization, signatures are obtained at each encounter. However, HCFA officials told us that the agency does not require managed care plans to provide a Privacy Act notification for the 15 percent of Medicare beneficiaries enrolled in them. HCFA officials told us that, since all Medicare+Choice beneficiaries must also be enrolled in Medicare Parts A and B, HCFA relies on the Medicare Parts A and B enrollment notices as the primary vehicles through which these beneficiaries learn about Privacy Act requirements.

Some of the HCFA Privacy Act notification forms we reviewed contain the required information; others do not tell beneficiaries the purposes for which their information may be disclosed outside of HCFA, or do so in an unclear fashion. For example, a form for beneficiaries receiving services in skilled nursing facilities provided the required information by advising beneficiaries why the information was being collected, and when the personally identifiable information could be disclosed outside the agency under the Privacy Act's routine uses provision. It clearly advised that the information collected during a nursing home stay would be used to track changes in health and functional status over time to evaluate and improve the quality of care provided by nursing homes that participate in Medicare. In contrast, we found that the wording of the Privacy Act notice for the Medicare Enrollment Form for Part B services was cursory at best. The Part B form did not identify the routine uses that would be made of the beneficiary's information. It provided only a vague reference to the Federal Register as a source for such information, and failed to provide specifics to help beneficiaries locate relevant sections of the Federal Register. We also found problems in a form used to collect information on ESRD beneficiaries; this form did not mention routine uses for the information collected and did not refer beneficiaries to sources that could provide this information.

Inadequate HCFA Safeguards Could Compromise Confidentiality

HCFA's safeguards for protecting the confidentiality of Medicare beneficiaries' health information are inadequate. Several audits conducted by the OIG point out weaknesses in how HCFA safeguards electronic information. In addition, HCFA has conducted only limited reviews of safeguards used by carriers and fiscal intermediaries in the last 2 years, and does not routinely monitor the confidentiality protections of other organizations receiving personally identifiable Medicare information. HCFA

officials told us they are in the process of taking action to correct the weaknesses identified by the OIG. However, consistent with priorities established by OMB, HCFA has a moratorium on software and hardware changes until it is compliant with Year 2000 computer requirements.

HCFA Systems Security Manual Generally Follows OMB Guidance for Safeguarding Electronic Information

Under the Privacy Act, HCFA must establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records. OMB Circular A-130 provides agencies with guidance for safeguarding federal information resources, including paper and electronic records. Appendix III of the 1996 Circular provides detailed guidance on safeguarding electronic records and on management controls, such as assignment of responsibility for security, the development of a security plan, and ongoing review of security controls. It notes that a security plan should include mandatory periodic training in computer security and restricting users to the minimum access or type of access necessary to perform their jobs. A security plan is also expected to outline techniques for safeguarding the security of information and to establish a formal mechanism for responding to intruders or other incidents that can compromise the security of a computer system. HCFA's systems security manual generally adheres to OMB's guidance for safeguarding electronic information. In addition, HCFA's policy for Internet usage requires encryption to protect data. It calls for authentication or identification procedures to ensure that both the sender and the recipient are known to each other and are authorized to receive and decrypt such information.

Problems With HCFA Safeguards Over Electronic Information

HHS' OIG has identified control weaknesses in HCFA's safeguarding of confidential information.[8] The OIG's audits of fiscal years 1997 and 1998 financial statement audits identified a variety of problems with safeguards for electronic information at HCFA's central office and for selected Medicare contractors. The OIG reported that HCFA needs to implement an overall security structure to achieve security program objectives and discussed weaknesses in computer access controls (techniques to ensure that only authorized persons access the computer system), segregation of

[8]HHS/OIG, Report on the Financial Statement Audit of the Health Care Financing Administration for Fiscal Year 1996 (CIN: A-17-95-00096, July 17, 1997); HHS/OIG, Report on the Financial Statement Audit of the Health Care Financing Administration for Fiscal Year 1997 (CIN: A-17-97-00097, Apr. 24, 1998); and HHS/OIG, Report on the Financial Statement Audit of the Health Care Financing Administration for Fiscal Year 1998 (CIN: A-17-98-00098, Feb. 26, 1999). See also Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, Sept. 23, 1998). In February 1997, we designated information security as a high risk government operation. Government operations have been identified as high risk because of their greater vulnerabilities to waste, fraud, abuse, and mismanagement. See also High-Risk Series, An Update (GAO/HR-99-1, Jan. 1999).

duties (the division of steps among different individuals to reduce the risk that a single individual could compromise security), and service continuity (the ability to recover from a security violation and provide service sufficient to meet the minimal needs of users of the system). The OIG also reported problems with controls over operating system software integrity and application development and change controls. System software controls are critical in preventing unauthorized and authorized users from circumventing security controls that permit an organization to monitor access to systems programs and files. Application development and change controls ensure that only authorized programs and modifications are implemented. Without proper controls, there is a risk that security features could be omitted or turned off—either inadvertently or deliberately.

As part of its work at 12 Medicare contractors for the fiscal year 1998 financial statement audit, the OIG noted that auditors were able to penetrate security and obtain access to sensitive Medicare data at five Medicare contractors. The auditors' ability to do so without using their formal access privileges is of particular concern because unauthorized users can exploit this security weakness and compromise confidential medical data in several ways—for example, unauthorized individuals could be reading confidential data, disclosing it to others, and tampering with it.[9]

HCFA officials told us that they are in the process of taking actions to address the OIG's financial statement audit findings. However, HCFA's ability to make progress is currently affected by the agency's efforts to address Year 2000 computer requirements so that there will be no interruption of services and claims payments for beneficiaries and providers. To be consistent with priorities established by OMB, HCFA has established a moratorium on software and hardware changes because of the need for compliance with Year 2000 requirements.[10] During its fiscal year 1999 financial statement audit, the OIG will evaluate the effectiveness of any corrective actions HCFA is able to implement.

[9]See also Financial Audit: 1998 Financial Report of the United States Government (GAO/AIMD-99-130, Mar. 31, 1999) and Auditing the Nation's Finances: Fiscal Year 1998 Results Highlight Major Issues Needing Resolution (GAO/T-AIMD-99-131, Mar. 31, 1999).

[10]See Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999) and Year 2000 Computing Crisis: Readiness Improving But Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-99-50, Jan. 20, 1999).

HCFA Does Not Systematically Monitor How Organizations Protect Data Confidentiality

Although HCFA has a process for monitoring systems security at its claims administration contractors (carriers and fiscal intermediaries), HCFA officials told us that competing demands and resource constraints have prevented them from monitoring whether these organizations follow OMB guidance for protecting the confidentiality of information. In addition, HCFA officials told us that they do not check whether organizations outside of HCFA are complying with the requirements of their data use agreements to protect the confidentiality of personally identifiable information.

HCFA's regional offices have oversight responsibility for Medicare contractors. These offices are required to designate Systems Security Coordinators who (1) provide contractors with technical guidance as needed, (2) monitor compliance with systems security requirements, (3) report systems security problems and activities to the central office as needed, and (4) coordinate external audits and respond to findings. In addition, regional offices could potentially evaluate systems security through the Contractor Performance Evaluation (CPE) review process. CPE reviews are intended to evaluate Medicare contractors' compliance with Medicare laws and regulations.

HCFA officials told us that, other than OIG reviews, there were no explicit onsite reviews of contractors' security protections in fiscal years 1997 and 1998 because of resource constraints and the assignment of regional staff to assess contractor compliance with Year 2000 computer requirements. HCFA officials told us that they initiated reviews of network security in 1998 for 12 Medicare contracts at 4 of its 60 claims processing contractors.

HCFA officials also told us that they do not have a system for monitoring whether organizations outside of HCFA have established safeguards for personally identifiable health information received from the agency. When organizations sign data use agreements with HCFA, they agree to establish appropriate administrative, technical, and physical safeguards providing a level and scope of security not less than the level and scope of security established by OMB. HCFA relies on organizations to monitor their own compliance with the data use agreements.

Data use agreements include a requirement that those receiving information from HCFA use it only for its approved purpose. Researchers are not allowed to make subsequent use of data for a different purpose without obtaining new approval. An important provision of data use agreements requires the return or destruction of data upon completion of each project. HCFA officials told us that, in the past, they tracked the

expiration date of data use agreements to determine whether to follow up on the disposition of the data. HCFA officials stated that due to resource constraints, there is a backlog of about 1,400 expired data use agreements; users have not been contacted to establish whether they will return the data to HCFA or destroy them. HCFA officials said they plan to reduce the backlog by one-half by September 30, 1999, and continue to make progress on it thereafter. Although HCFA does not systematically monitor compliance with its data use agreements, HCFA officials told us that they scan Internet web sites to see if information is being disseminated without HCFA approval. In addition, they said HCFA staff review research journals and publications to determine if researchers have used HCFA data without appropriate authorization. However, such methods only identify problems after sensitive data have been inappropriately used, and do not assure comprehensive oversight of the use of these data. The lack of HCFA monitoring of contractors and others who use personally identifiable Medicare information hampers HCFA's ability to prevent the occurrence of problems and provide timely identification and corrective action for those that have occurred.

Few Complaints of Privacy Act Violations Reported

HCFA said it has received and resolved 7 complaints of potential Privacy Act violations in the past 4 years. Six of the complaints involved contractors conducting research for HCFA, health data organizations, and individual researchers. The complaints were made by similar organizations or other researchers and involved potentially identifiable Medicare billing information posted on an Internet web site, data obtained for one research project used and published for a second without authorization from HCFA, and offers to share Medicare files at a national research conference. In these cases, HCFA provided direction to those involved to clarify and further sensitize researchers to Privacy Act requirements.

The seventh complaint was brought against HCFA and an individual researcher by a Medicare beneficiary. The Secretary of HHS received a complaint letter from an attorney representing a Medicare beneficiary who objected to two letters sent to her by a researcher from a major university medical school. The letters asked her to participate in a followup study of Medicare patients who had undergone a particular surgical treatment for heart disease. The beneficiary believed that the letters implied she was under an obligation to participate in the study and wanted to know how her medical history had been shared with the researcher. HCFA determined that its data on this beneficiary and others had been released to the researcher. While HCFA determined that appropriate data use agreements

had been signed for both sets of data, the investigation also showed that the letters sent by the researcher may have been worded too strongly. In addition, the researcher failed to follow the HCFA notification procedure; instead of sending out the HCFA Administrator's letter in advance of his own mailing, he merely attached it to his first letter to the beneficiary. HCFA sent a letter to the beneficiary's attorney to explain the legal basis for the disclosure of the beneficiary's information and to advise that participation in such research is completely voluntary. The letter also indicated that HCFA had taken steps to ensure that the beneficiary would not be contacted for further studies. HCFA received no further correspondence from the beneficiary or her attorney on this matter.

We found no lawsuits related to the Privacy Act brought by Medicare beneficiaries against HCFA, nor from our discussions with HCFA officials are we aware of any cases settled prior to or during litigation. Similarly, we found no evidence of criminal prosecutions for Privacy Act violations at HCFA.

HCFA reports that only one internal disciplinary action related to violations of HCFA's confidentiality policies has occurred during the past 5 years. The incident involved an agency employee who was accessing beneficiary files more frequently than appeared necessary for performing his job functions. The employee admitted to looking at the files of famous people and was placed on administrative leave. He eventually signed an affidavit stating that the files had not been sold or shared with other persons and he was accordingly allowed to resign.

HCFA staff stated that HCFA has never terminated or modified a contract in response to a claims administration contractor's breach of Privacy Act standards. However, HCFA officials reported that, in 1997, it received a report from one of its contractors that the contractor's director of Medicare payment safeguards had taken a file from the workplace and shared it with her spouse, a doctor employed by the contractor as part of its private line of business. The file concerned an active fraud investigation of another doctor. According to HCFA, the contractor issued a letter of corrective action to remain in the employee's record for 1 year.

Some States Restrict Disclosure of Sensitive Confidential Information

In its oversight of the Medicare program, HCFA necessarily deals with beneficiaries and providers from every state. The states have laws governing the confidentiality of health information which vary significantly, resulting in what has been called a patchwork system of protections. For example, in Minnesota, health records generally may not be disclosed by a provider without a patient's consent. While an exception is made for records used in research, any release for research purposes requires, among other things, that the provider attempt to acquire a patient's consent and determine that individually identifiable records are necessary, the researcher's safeguards are adequate, and the researcher will not use the records for purposes other than the original request without the patient's consent. In Florida, mental health records are confidential and may be disclosed only under limited circumstances. In Vermont, all individually identifiable information reported to the state's cancer registry, used in cancer morbidity and mortality studies, is confidential and privileged and may be used only for the purposes of these studies.

In an effort to establish some degree of national uniformity, HIPAA requires that, unless the Congress enacts a health privacy law establishing standards for the electronic exchange of information by August 21, 1999, the Secretary of HHS must promulgate such standards by regulation within the following 6 months. The proposals Congress is considering differ in the extent to which federal privacy protections would preempt state laws.

Conflicts between HCFA and the states involving medical record disclosures have been minimal, according to HCFA officials, and HCFA's administration of the Medicare program has not been hindered because HCFA officials believe all states permit information to be released as needed for health care treatment and payment. If a state law prohibited disclosure of information to HCFA that was critical for treatment or payment purposes, and a federal statute required such disclosure, HCFA officials told us that it would rely on the Supremacy Clause of the U.S. Constitution[11] and its express statutory authority to obtain the necessary records.

If information is not critical to HCFA operations, HCFA officials told us, HCFA policy is to respect and abide by state laws that provide greater protection for records than federal law or regulation. For example, when the states of

[11]U.S. Const. art. VI, cl. 2. The Supreme Court has construed the Supremacy Clause of the U.S. Constitution to hold that federal law preempts state law where, for example (1) the state law directly conflicts with federal law, (2) the federal legislative scheme leaves no room for state regulation, or (3) the state statute frustrates or conflicts with the purposes of the federal law.

California and Washington notified HCFA that their state laws did not authorize the disclosure of diagnostic information related to HIV/AIDS and STDs, HCFA changed the system used to collect and analyze certain nursing home information by allowing states to withhold diagnostic information collected about their nursing home patients concerning HIV/AIDS and STDs.[12] HCFA officials told us that 15 states have exercised this option by blanking out HIV/AIDS or STD identifiable codes before submitting the requisite information to HCFA.

According to HCFA officials, the deletion of diagnostic information collected about nursing home patients concerning HIV/AIDS and STDs has not generally affected its operations. They said that when the agency developed its prospective payment system for skilled nursing facilities, it did not use data on beneficiaries with HIV/AIDS and STDs in nursing homes to set nursing home payment rates. Since HCFA began phasing in the skilled nursing facility prospective payment system in 1998, however, it has received requests for additional payment from providers who care for HIV/AIDS patients. HCFA officials acknowledge that it now needs better information on this population as it refines the new payment system for skilled nursing facilities to ensure that beneficiaries with HIV/AIDS receive the level of care required and that rates are adequate to provide for that care. Similarly, HCFA officials told us that the agency will require diagnostic information as it refines its other payment systems.

Conclusions

In its role as administrator and overseer of the nation's Medicare program, HCFA must collect and maintain personally identifiable information on millions of beneficiaries to effectively operate and manage the program. In addition, HCFA and others require this information for essential research activities that can lead to improvements in the nation's health care access, financing, and quality. As the steward of this confidential information, HCFA must balance privacy concerns of beneficiaries with its need to effectively manage the program. It must protect individuals' health information from inappropriate disclosure.

In carrying out this responsibility, HCFA has policies and practices that are generally consistent with the Privacy Act and OMB guidance to reduce the likelihood of inappropriate or inadvertent disclosures. In addition, HCFA's protections may be strengthened by its recent establishment of a Beneficiary Confidentiality Board and actions taken in response to OMB

[12]The information is used by HCFA to track changes in health and functional status of nursing home residents. The information system is known as the National Minimum Data Set (Resident Assessment Instrument) repository.

guidance to reevaluate the relevance and necessity of maintaining personally identifiable information. However, as the OIG reported, HCFA's information management systems continue to have vulnerabilities. In addition, HCFA has not consistently monitored its contractors' safeguards for protecting confidential information. As a result, even though few complaints have been made to date, confidential medical information may be at risk. To be consistent with priorities set by OMB, HCFA has focused its resources on ensuring that the agency and its contractors are compliant with year 2000 computer requirements. Nonetheless, we believe that reducing the vulnerabilities in its information systems and contractor monitoring are important concerns that HCFA must address.

HCFA cannot readily provide beneficiaries with an accounting of disclosures of information about them. The agency is also unable to inform oversight agencies about certain Privacy Act activities. In addition, HCFA does not have a formal system for monitoring organizations to whom it discloses personally identifiable information. As a result, after data are released to an organization, HCFA is unable to systematically reduce the likelihood of inappropriate data use or identify instances of such misuse.

HCFA can also do a better job of informing beneficiaries that their information could be disclosed. In addition, the agency should be better able to track and report disclosures of Medicare records. Notification is also inadequate. When new information is collected from beneficiaries and they are notified of their rights under the Privacy Act, some of HCFA's notifications do not clearly tell Medicare beneficiaries the purposes for which their information may be disclosed outside of HCFA.

If HCFA were restricted from receiving uniform health information from across the country, internal operations such as rate-setting and monitoring for quality assurance could be adversely affected. It could also affect the ability of analysts in HCFA, other federal agencies, and nongovernmental organizations to conduct policy analysis and health services research because of the difficulty of complying with varying state laws. If the same data elements and health information were not available from all states, HCFA's ability to conduct research and analysis to improve Medicare policies may be compromised.

Recommendations

To improve HCFA's protection of the confidentiality of personally identifiable Medicare beneficiary information, we recommend that the Administrator (1) correct the vulnerabilities identified in its information

management systems by the OIG; (2) systematically monitor contractors' safeguards for protecting confidential information; (3) develop a system to routinely monitor other organizations that have received personally identifiable information on Medicare beneficiaries to help ensure that information is used only as approved and to identify instances of misuse; (4) ensure that all agency Privacy Act notifications convey the information required by the Act in a manner that is clear and informative to beneficiaries; and (5) implement a system that would permit HCFA to respond in a timely fashion to beneficiary inquiries about the disclosure of their information to others outside HCFA as well as to provide information on Privacy Act activities to OMB and others.

Agency Comments

In a July 16, 1999, letter in response to a draft of this report, HCFA concurred with our recommendations (see appendix II). HCFA said that it recognizes its responsibility to protect the confidentiality of beneficiary information and that it has policies and procedures to comply with the provisions of the Privacy Act. However, it added that it could improve the existing mechanisms for ensuring confidentiality. HCFA said that its recently established Beneficiary Confidentiality Board is charged with reviewing all existing HCFA policies and procedures governing the release of Medicare data and developing new policies and procedures, where necessary, to ensure the confidentiality of patient-identifiable health information.

Specifically, HCFA concurred with our recommendations to correct the vulnerabilities identified by the OIG in its information management system and to systematically monitor contractors' safeguards for protecting confidential information. HCFA identified initiatives it has undertaken, stated that progress has been made in many areas, and said that it will intensify its efforts to put in place a comprehensive security initiative when resources are freed from its efforts to address year 2000 computer requirements. It also said that it is planning to incorporate security oversight into its contractor performance evaluation efforts. While we support all of these actions, we believe it is essential that HCFA evaluate the effectiveness of any corrective actions it is able to implement.

HCFA also concurred with our recommendation to develop a system to routinely monitor other organizations that have received personally identifiable information to help ensure that information is used only as approved and to identify instances of misuse. HCFA identified steps it is taking to improve the process for monitoring how other entities use

confidential Medicare information. It said it is reviewing all of its data disclosure procedures, exploring best practices of other agencies, and developing recommendations to expand the role of the data custodian within the organization that receives confidential information. In addition, it is reviewing the feasibility of annually renewing data use agreements and increasing its follow-up effort with researchers to verify they have complied with data use agreements. We support all of these initiatives. However, we believe HCFA should also examine the feasibility of expanding its verification of compliance with data use agreements to all organizations receiving confidential Medicare information and not limit its verification to research organizations.

In regard to Privacy Act notifications, HCFA concurred with our recommendation that the notifications contain the information required by the Act in a manner that is clear and informative to beneficiaries. It said that improving the forms will be a priority and it has begun action to improve existing notices and ensure that new notices contain the required Privacy Act information in a form understandable to beneficiaries. We believe that implementation of these actions may better ensure that Medicare beneficiaries understand how their personal health care information might be used.

HCFA also concurred with our recommendation to implement a system that would permit it to respond in a timely fashion to beneficiary inquiries about the disclosure of their information to others outside of HCFA as well as to provide information on Privacy Act activities to OMB. HCFA said it will develop a system to respond to beneficiaries' requests about the disclosure of their information. It also said that it is developing a new tracking system to create reports responsive to OMB and Privacy Act reporting requirements.

HCFA also provided technical comments, which we incorporated where appropriate.

We are sending copies of this report to other interested congressional committees, the Honorable Donna E. Shalala, Secretary of Health and Human Services; the Honorable Nancy-Ann Min DeParle, Administrator of HCFA; and other interested parties. We will also make copies available to others upon request.

Please contact me at (312) 220-7600 if you or your staff have any questions concerning this report. Staff contacts and other contributors are listed in appendix III.

Sincerely yours,

Leslie G. Aronovitz
Associate Director
Health Financing and Public Health Issues

Contents

Abbreviations

AIDS	acquired immunodeficiency syndrome
CPE	Contractor Performance Evaluation
ESRD	end-stage renal disease
HCFA	Health Care Financing Administration
HHS	Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIV	human immunodeficiency virus
OIG	Office of Inspector General
OMB	Office of Management and Budget
STD	sexually transmitted disease

Scope and Methodology

We focused our work at HCFA on controls over the disclosure of personally identifiable information involving Medicare beneficiaries. We interviewed agency officials and reviewed documents they provided, including HCFA policies and procedures related to safeguarding and disclosing personally identifiable health information. We also reviewed OMB guidance related to the Privacy Act. We reviewed financial statement audits of HCFA from HHS' OIG, the HHS financial management fiscal year 1998 status report and 5-year plan, and court cases related to the Privacy Act. In addition, we examined the privacy protections of selected state laws and obtained comments from agency officials about the current and future effect of such laws on HCFA's management of the Medicare program. We conducted our work from April through June 1999 in accordance with generally accepted government auditing standards.

Comments From the Health Care Financing Administration

DEPARTMENT OF HEALTH & HUMAN SERVICES

Health Care Financing Administration

Deputy Administrator
Washington, D.C. 20201

JUL 16 1999

FROM: Michael M. Hash
Deputy Administrator, HCFA

SUBJECT: General Accounting Office (GAO) Draft Report, "Medicare: Improvements Needed by HCFA to Enhance Protection of Confidential Health Information"

TO: Leslie Aronovitz, Associate Director
Health Financing and Public Health Issues, GAO

We appreciate the opportunity to review your draft report to Congress concerning the confidentiality of personally identifiable health information for Medicare beneficiaries. Please find our comments attached.

This Administration has been firmly committed to protecting medical privacy. HCFA provides much greater protection for such information than the private sector and we strive to continually enhance those protections. In this context, we especially appreciate the work that has gone into this study.

HCFA recognizes its responsibility to protect the confidentiality of beneficiary information and has in place policies and procedures to comply with the provisions of the Privacy Act. Recognizing, as GAO has pointed out, there is room for improving the existing mechanisms for ensuring confidentiality, HCFA has already taken several substantial steps that will help to address the GAO recommendations. For example, we hired outside experts to identify and help correct potential security weaknesses in our systems, acquired new technology, and enhanced procedures for guarding access to sensitive information. Moreover, we are currently reviewing all of our existing data disclosure procedures and have established a Beneficiary Confidentiality Board to review all existing HCFA policies and practices concerning the release of Medicare data.

As pointed out in the report, personally identifiable information on Medicare beneficiaries is essential to ensure beneficiaries get the quality care that they need, and to exercise effective stewardship of the Medicare program and maintain the public trust. We will continue to monitor this situation carefully and to make improvements as needed. Protecting the confidentiality of information on Medicare beneficiaries while simultaneously utilizing this data to perform essential Medicare research remains one of our highest priorities.

Attachment

Comments of the Health Care Financing Administration (HCFA)
on the General Accounting Office (GAO) Draft Report,
"Medicare: Improvement Needed by HCFA to
Enhance Protection of Confidential Health Information"

Overview

Personally identifiable information on Medicare beneficiaries is essential to the operation of the Medicare program. It is an invaluable asset in our efforts to improve care and coverage for beneficiaries. We need it to ensure beneficiaries get quality care, make payment, coordinate benefits, project spending, develop and refine policy, assess quality and access to care, fight fraud, waste and abuse, and be responsive to individual beneficiary inquiries.

HCFA recognizes its responsibility to protect the confidentiality of beneficiary information. HCFA has in place policies and procedures to comply with the provisions of the Privacy Act. As GAO has pointed out, there is room for improving the existing mechanisms for ensuring confidentiality.

Protecting the confidentiality of our beneficiaries health information is a critical task, which has become even more important in recent years because of the new technological environment. Recognizing the ever-increasing difficulty of protecting the confidentiality of HCFA records in this new environment, HCFA recently established a Beneficiary Confidentiality Board, comprised of senior executives to review all existing HCFA policies and procedures governing the release of Medicare data and to develop new policies and procedures, where necessary, to ensure the continued confidentiality of patient identifiable health information.

In addition, HCFA has developed an enterprise-wide systems security initiative to strengthen protection measures discussed more fully below.

GAO Recommendation

To improve HCFA's protection of the confidentiality of personally identifiable Medicare beneficiary information, we recommend that the HCFA Administrator:

-- Correct the vulnerabilities identified in its information management systems by the OIG

HCFA Comment

We concur with the GAO recommendation. One of the first actions our Chief Information Officer, Gary Christoph, took when he came on board was to hire outside experts to search out potential security weaknesses in our systems so we could proactively address them. We have

acquired new technology, enhanced staff training, conducted our own risk assessments and internal audits, and enhanced procedures for guarding access to sensitive systems. There are no "silver bullets"; vigilance here must be constant, given the ever changing nature of technology and evolution of risks.

The findings of our own assessments as well as the findings and recommendations cited by the OIG and the GAO, have shaped our enterprise-wide security initiative. The initiative has four elements: policies and procedures, training, systems engineering, and oversight and management. Although we have been able to initiate some actions on this initiative, we are prepared to aggressively move with its implementation as we clear the Y2K hurdle.

HCFA has taken a number of steps since the OIG review, while also conducting Y2K work. Even though the 1997 and 1998 audits were performed in close proximity and it was difficult to address many of the early findings, the auditors found that some of the previous findings could be closed and that progress had been made in many areas. Examples of that progress follow.

+ HCFA has significantly strengthened its central security management capability. We reorganized to create a Security and Standards Group. Its operations closely follow the principles outlined in GAO's Executive Guide to Information Security Management.
+ All new major application systems must have a security plan and we have hired a contractor to perform Independent Verification and Validation (IV&V) on each plan. After Y2K, we will address legacy systems.
+ All new security plans are accompanied by a certification by responsible component technical and managerial staff.
+ Our formalized awareness and training plan have been completed.
+ HCFA worked aggressively to address the material weakness in our legacy database management system. HCFA successfully negotiated with our contractor to develop and include an enhanced protection mechanism into its product. HCFA worked with the contractor to independently validate the identified solution.

We believe we have put in place a comprehensive security initiative that will take it into the 21st century. As resources are freed from Y2K, we will be able to intensify our efforts in implementing this initiative. The President's FY2000 Budget request includes significant funding to improve the data security systems for DHHS.

GAO Recommendation

-- Systematically monitor contractors' safeguards for protecting confidential information

HCFA Comment

We concur with the GAO recommendation. Since 1994, HCFA has had in place Medicare contractor guidelines which require fiscal intermediaries and carriers to establish and maintain security protections, as required by OMB Circular A-130. In 1998, HCFA conducted independent reviews of network security of 12 Medicare contractors at four sites while also performing extensive Y2K preparations. We have been working with other oversight organizations (e.g., OIG, IRS, and GAO) to perform safeguard reviews.

Oversight efforts of the Medicare contractor operations are a key element of the enterprise-wide security initiative discussed above. The oversight efforts will include: review of security plans, tracking corrective actions, and EDP control assessments. We are planning to incorporate security oversight into our contractor performance evaluation efforts.

GAO Recommendation

-- Develop a system to routinely monitor other organizations that have received personally identifiable information on Medicare beneficiaries to help ensure that information is used only as approved and identify instances of misuse

HCFA Comment

We concur. HCFA will continue to improve the process for monitoring how other entities use confidential Medicare data.

HCFA is required to collect patient-level data on all Medicare beneficiaries in order to administer the Medicare program. In conducting its main business functions of paying claims, ensuring quality of health care, defining covered services, and improving payment systems, HCFA, when necessary, utilizes the services of outside experts. While these support organizations may receive temporary access to Medicare data, anyone who violates the Privacy Act could face fines and imprisonment. Whenever an outside group has access to Medicare person-identifiable data, HCFA endeavors to ensure that patient confidentiality is maintained at all times and that the data are only used for a specific purpose.

For all requests for beneficiary identifiable information, HCFA conducts a careful review to ensure that the disclosure of information is allowed under the Privacy Act. For requests from organizations outside of DHHS we conduct another careful level of review to ensure that the purpose for the disclosure is consistent with the reason for which the data were collected. HCFA's practice is to provide the bare minimum of information that is essential to accomplish the given purpose. HCFA is also diligent in making clear to requestors how data that could be used to identify individual beneficiaries must be protected.

HCFA staff are currently reviewing all of the existing data disclosure procedures. In addition, HCFA staff are consulting with other Federal agencies to explore "best practices" of how they monitor the release of person-identifiable data to ensure that the information is only used for the specific purposes for which it was approved. HCFA staff are developing recommendations which will be submitted to the Beneficiary Confidentiality Board which will expand the role and responsibilities of the "data custodian" within the organization that receives the data. Currently, every requestor signs a data use agreement, in which the data requestor pledges to protect the confidentiality of Medicare data. This document also identifies a data custodian that is responsible for monitoring all usage of the data. We will recommend that the Beneficiary Confidentiality Board require the data custodian submit to HCFA bi-monthly reports which identify everyone who had access to the Medicare data and how the data are being used. In addition, the custodian will report on the status of any articles, reports or other public disclosures of summary data which is derived from the person identifiable data. We are also reviewing the feasibility of requiring that the data use agreement be renewed annually. Finally, we are also increasing efforts to follow-up with researchers to verify that they have in fact complied with their data use agreements to protect data and dispose of it properly once their projects are completed.

GAO Recommendation

-- Ensure that all Privacy Act notifications contain the information required by the Act in a manner that is clear and informative to beneficiaries

HCFA Comment

We concur with the GAO recommendation. We agree entirely that all of our Privacy Act notifications need to contain the statutorily prescribed information in a form that is clear and useful to beneficiaries. By law such notices need to include the authority for the information collection, the intended principal purposes for which the information is to be collected, the routine uses of the information which may be made, and whether the information collection is voluntary or mandatory and how not providing information will affect an individual.

Our most recent Privacy Act notice, for beneficiaries in home health care settings (i.e., the Outcome and Assessment Information Set (OASIS)), not only provides all the required information, it is written in much plainer language to be clear and as informative as possible to beneficiaries. Additionally, it includes, on its reverse side, a substantially simplified notice in plain language which we believe will greatly enhance beneficiary understanding of the key messages of the Privacy Act notification.

Improving existing Privacy Act notices which do not currently meet such standards is a priority action. Earlier this year, HCFA began a concerted effort to formulate organizing principles and a coherent communication plan for the agency's notices, and to improve existing notices to meet current standards and requirements for notices which are simplified, beneficiary-friendly, plain

language, culturally competent, literacy-sensitive, accurate, timely, and effective. HCFA staff specializing in consumer protections are developing content validation processes to ensure that new notices, and deficient existing notices, meet these standards and requirements. Improvement of the forms which the Report specifies as deficient will be a priority for HCFA.

GAO Recommendation

-- Implement a system that would permit HCFA to respond in a timely fashion to beneficiary inquiries about the disclosure of their information to others outside of HCFA as well as to provide information on Privacy Act activities to OMB and others.

HCFA Comment

We concur. Although we have not received any such requests, we recognize that the Privacy Act requires this capability. Fully defining the requirements and designing efficient information systems to ensure full compliance with these requirements is a significant information technology priority for the Agency. HCFA will put procedures in place to respond to inquiries that occur while developing those requirements.

To improve HCFA's reporting mechanism for Privacy Act activities, HCFA is currently developing a new tracking system that will be able to create reports responsive to OMB and Privacy Act reporting requirements; e.g., disclosures by System of Record will be readily identifiable.

GAO Contacts and Staff Acknowledgments

GAO Contacts

Leslie G. Aronovitz, (312) 220-7600
Bruce D. Layton, (202) 512-6837

Staff Acknowledgments

In addition to those named above, Nancy Donovan, Bonnie L. Brown, Nila Garces-Osorio, Julian Klazkin, Mary Reich, and Craig Winslow made key contributions to this report.

Related GAO Products

Year 2000 Computing Challenge: Estimated Costs, Planned Uses of Emergency Funding, and Future Implications (GAO/T-AIMD-99-214, June 22, 1999).

Year 2000 Computing Crisis: Readiness of Medicare and the Health Care Sector (GAO/T-AIMD-99-160, Apr. 27, 1999).

Financial Audit: 1998 Financial Report of the United States Government (GAO/AIMD-99-130, Mar. 31, 1999).

Auditing the Nation's Finances: Fiscal Year 1998 Results Highlight Major Issues Needing Resolution (GAO/T-AIMD-99-131, Mar. 31, 1999).

Medical Records Privacy: Access Needed for Health Research, but Oversight of Privacy Protections Is Limited (GAO/HEHS-99-55, Feb. 24, 1999).

Year 2000 Computing Crisis: Readiness Improving, but Much Work Remains to Avoid Major Disruptions (GAO/T-AIMD-50, Jan. 20, 1999).

Major Management Challenges and Program Risks: Department of Health and Human Services (GAO/OGC-99-7, Jan. 1999).

Medicare Computer Systems: Year 2000 Challenges Put Benefits and Services in Jeopardy (GAO/AIMD-98-284, Sept. 28, 1998).

Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92, Sept. 23, 1998).

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 37050
Washington, DC 20013

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 (202) 512-6061, or TDD (202) 512-2537.

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

or visit GAO's World Wide Web Home Page at:

http://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