OFFICE OF
THE INSPECTOR GENERAL

SOCIAL SECURITY ADMINISTRATION

HOSPITALS' USE AND PROTECTION OF SOCIAL SECURITY NUMBERS

January 2006 **A-08-06-16056**

AUDIT REPORT

Mission

We improve SSA programs and operations and protect them against fraud, waste, and abuse by conducting independent and objective audits, evaluations, and investigations. We provide timely, useful, and reliable information and advice to Administration officials, the Congress, and the public.

Authority

The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

To ensure objectivity, the IG Act empowers the IG with:

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

Vision

By conducting independent and objective audits, investigations, and evaluations, we are agents of positive change striving for continuous improvement in the Social Security Administration's programs, operations, and management and in our own office.

SOCIAL SECURITY

MEMORANDUM

Date: January 27, 2006 Refer To:

To: The Commissioner

From: Inspector General

Subject: Hospitals' Use and Protection of Social Security Numbers (A-08-06-16056)

OBJECTIVE

Our objective was to assess hospitals' use and protection of Social Security numbers (SSN) and the potential risks associated with such use.

BACKGROUND

Hospitals admit thousands of individuals each year. To assist in this process, and for other purposes, many hospitals use patients' SSNs. Although no single Federal law regulates overall use and disclosure of SSNs, the *Social Security Act* and the *Privacy Act of 1974* contain provisions that govern disclosure and use of SSNs. Additionally, the *Health Insurance Portability and Accountability Act of 1996* addresses the privacy and security of all "individually identifiable health information." See Appendix A for more information on the specific provisions of these laws.

We selected a sample of 10 hospitals nationwide. For each selected hospital, we interviewed hospital personnel and reviewed hospital policies and practices for using and protecting SSNs. See Appendices B and C for additional details regarding our scope and methodology and hospitals we visited, respectively.

RESULTS OF REVIEW

Based on our interviews with hospital personnel and reviews of hospital policies and practices, we are concerned about hospitals' use and protection of SSNs. Despite the increasing threat of identity theft, some hospitals used SSNs as patient identifiers or for other purposes, even when another identifier would suffice. In addition, some hospitals unnecessarily displayed SSNs on documents that may have been viewed by hospital personnel, some of whom may not have had a need to know. Based on our previous audit and investigative findings, we know that unnecessary access, disclosure, and use of SSNs increase the potential for dishonest individuals to obtain these numbers and misuse them, thus creating SSN integrity issues. Some hospital personnel with whom we spoke shared our concern and were taking steps to limit SSN use.

HOSPITALS' USE OF SSNs IS WIDESPREAD

Hospitals primarily used SSNs for internal administrative purposes, such as admitting, registering, billing, insurance, and research. Although the hospitals generally used patient medical record numbers as primary identifiers, they also used SSNs as a secondary identifier. Hospitals also collected and used SSNs to verify patients' eligibility or insured status because some government benefit providers (that is, Medicare/Medicaid) and health insurance companies use SSNs as primary identifiers and display the number on their members' identification cards. Most hospital officials told us they use SSNs because each is unique to an individual and does not change like other identifiers. This is particularly vital in a hospital setting, given the importance of tracking patients' medical records among multiple health care providers. However, officials at all of the hospitals we visited told us that, if patients did not provide their SSN, the hospital assigned them an alternate number.

One hospital official told us his facility displays SSNs on the wristbands of those patients whom the hospital admitted before 1999. However, this practice does not apply to new patients or patients the hospital admitted in 1999 or later. The hospital assigns these individuals a machine-generated medical record number, which is displayed on patients' wristbands. Displaying SSNs on patient wristbands allows countless individuals the opportunity to view patients' SSNs, unnecessarily subjecting them to the possibility of identity theft.

Hospitals also provided patient SSNs to external entities. That is, hospitals provided SSNs to third parties, such as researchers, contractors, insurance companies, and other medical providers. They also provided patient SSNs to various Federal and State agencies for health statistics and registries. In addition, hospitals used SSNs to track patients' medical records among multiple providers, which helped identify patients' medical histories.

The executive director of a large health information association told us that almost all hospitals include SSNs as one element of their patient's identity file (that is, secondary

identifier). She estimated that about 5 percent (about 288) of hospitals nationwide use SSNs as primary patient identifiers. According to this official, patients' SSNs are generally displayed on every page of a paper record, every screen of an electronic record, and the key field in all databases. Furthermore, patients' SSNs are available to anyone who might obtain copies of the patient's medical record.

HOSPITALS PLACE CONTROLS OVER PATIENT INFORMATION BUT DISPLAY SSNs ON DOCUMENTS THAT MAY BE VIEWED BY INDIVIDUALS WITHOUT A NEED TO KNOW

Hospitals had some controls in place to safeguard patient information, including SSNs. For example, hospitals (1) limited physical and electronic access to computers and information systems, (2) shredded documents that contained personal identifying information, and (3) conducted self-reviews to ensure compliance with policies and procedures. In addition, hospitals entered into business associate agreements with third parties that contained specific language related to personal information safeguards.

While delivering medical services, however, some hospitals displayed SSNs on documents that may have been viewed by others, some of whom may not have had a need to know. We identified numerous instances in which hospital personnel, such as doctors, nurses, laboratory technicians, dieticians, and social service personnel, had access to medical records containing patients' SSNs. We question whether these individuals need to know a patient's SSN. We also identified instances in which hospital personnel displayed SSNs on data it sent to third parties/independent contractors, such as consultants who provided systems and technical support. We question whether these third parties need to know a patient's SSN.

We believe displaying SSNs on documents (paper or electronic) that may be viewed by hospital personnel or third parties who may not have a need to know increases the risk that others may improperly obtain and misuse the SSN. In fact, hospital officials acknowledged the potential risks for identity theft and fraud, and one director of hospital operations told us he plans to recommend that patients' SSNs be limited to only those personnel who have a business need to know.

POTENTIAL RISKS ASSOCIATED WITH COLLECTING AND USING SSNs

Hospitals' collection and use of SSNs entail certain risks. Each time an individual divulges his or her SSN, the potential for someone to illegally gain access to personal identifying information increases. For example, an employee at 1 hospital we visited stole the SSNs and other personal identifying information from document labels on 13 patients' medical records. Hospital officials told us they recognized the vulnerability associated with displaying SSNs on document labels and discontinued this practice. Because many hospitals still use SSNs as patient identifiers or for other purposes, patients' exposure to identity theft remains today. We believe the following examples illustrate patients' risk of exposure to such activity.

- Minnesota authorities convicted 2 hospital employees of stealing 32 patients' identities. The identity thieves used this information to open fraudulent credit card and telephone accounts and charge over $78,000. Both individuals were scheduled to be sentenced to serve a period of 4 to 6 months in a workhouse and render restitution. They are also prohibited from employment in which they would have access to confidential patient information.

- A man used the identities of four patients at a Connecticut hospital to purchase $6,000 in home improvement merchandise. Police believe the perpetrator obtained this information from his wife, who worked at a hospital. The man was charged with 79 counts of receiving goods and services from illegal use of a credit card, 36 counts of credit card crimes of possession, and numerous counts of larceny and identity theft.

- A hospital employee in Alabama earned $100 for each name and SSN she gave a buyer who used the numbers to file fraudulent tax returns. The victims were children.

- A nurse in Missouri was sentenced to 1 year and 1 day in Federal prison for stealing identity information of two patients. She admitted using her access to patient information to obtain credit accounts and make purchases on these accounts.

SOME HOSPITALS AND HEALTHCARE-RELATED ENTITIES ARE TAKING STEPS TO LIMIT SSN USE

Incidences of identity theft at hospitals and the recognition that SSNs are linked to vast amounts of personal information have led some hospitals to reconsider their use of SSNs. Several hospitals we visited are taking steps to limit SSN use. In addition, some healthcare-related entities have turned to alternate identifiers.

The director of health information services at one hospital and assistant administrator at another hospital told us their facilities plan to truncate patients' SSNs because of identity theft concerns. The director also told us his hospital received a significant number of patient and employee complaints regarding SSNs in its computer systems. The director told us his hospital is taking steps to identify (1) hospital personnel who need to know the entire SSN and (2) information system pathways that will be affected by the change. Both hospitals will continue to use patients' entire SSNs for billing and eligibility purposes because some health insurers and Medicare/Medicaid use SSNs as primary identifiers.

One large California health insurer we visited removed SSNs from member identification cards because the State enacted a law[1] restricting such activity. The health insurer created a unique number to identify members in its databases. Health

[1] California Civil Code § 1798.85 (2005).

insurer officials told us the company wanted to reduce its vulnerability to identity theft by reducing its reliance on SSNs as primary identifiers. In fact, most of its affiliated independent insurers have issued new identification numbers. In addition, a director with the Centers for Medicare and Medicaid Services told us the Agency is considering replacing SSNs with alternate identifiers because of increased identity theft and privacy concerns. According to the director, her agency is analyzing data to determine the types of information systems and work processes that would require revisions to accommodate such a change. Because Medicare/Medicaid use SSNs as primary identifiers and display the number on their members' identification cards, we will provide a copy of this report under separate cover to the U.S. Department of Health and Human Services' Inspector General.

A large health information management association we visited published best practice procedures for safeguarding SSNs. The association recommended that healthcare organizations "minimize the use of Social Security numbers for identification: whenever possible, redact or replace some of the digits in the Social Security number; avoid displaying the entire number on any document, screen, or data collection field." In addition, the association recommended that only "staff directly involved in patient registration, billing, collections and number reconciliations" should have access to SSNs. The association did not believe most hospital personnel, such as nurses, dieticians, radiologists, or pharmacists should have access to patients' SSNs.

CONCLUSION AND RECOMMENDATIONS

Despite the potential risks associated with using SSNs as patient identifiers, hospitals continue this practice. While we recognize the Agency cannot prohibit hospitals from using SSNs as patient identifiers, we believe it can help reduce potential threats to SSN integrity by encouraging hospitals to limit SSN collection and use. We also recognize the challenge of educating such a large number of hospitals. However, given the potential threats to SSN integrity, such a challenge should not discourage the Agency from taking steps to safeguard SSNs. Accordingly, we recommend that the Social Security Administration:

1. Coordinate with hospitals and relevant healthcare associations to educate hospitals about the potential risks associated with using SSNs as patient identifiers. For example, we believe the Agency should consider hosting or participating in conferences to discuss ways hospitals can enhance SSN integrity.

2. Encourage hospitals to limit their collection and use of SSNs. For example, we believe hospitals should safeguard patients' SSNs by limiting access to hospital personnel and external entities with a business need to know and avoid displaying the entire number on any document, screen, or data collection field.

3. Encourage the Centers for Medicare and Medicaid Services to remove SSNs from its identification cards and partner with them to develop an alternate identifier that meets both agencies needs.

4. Promote the best practices of hospitals that are taking steps to limit their use of SSNs. For example, the Agency could promote best practices through activities such as contributing articles to healthcare-related journals and association newsletters.

AGENCY COMMENTS AND OIG RESPONSE

SSA agreed with our recommendations. The Agency's comments are included in Appendix D.

Patrick P. O'Carroll, Jr.

Appendices

Federal Laws that Govern Disclosure and Use of the Social Security Number

The following Federal laws establish a general framework for disclosing and using the Social Security number (SSN).

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
(42 U.S.C. §§ 1320d-1320d-8; P.L. 104-191, §§ 261 – 264; 45 C.F.R. Parts 160 & 164)

HIPAA's Administrative Simplification provisions address the privacy and security of health data, including SSNs. HIPAA's Privacy Rule protects all *"individually identifiable health information"* held or transmitted by a covered healthcare entity or its business associate, in any form or media, whether electronic, paper, or oral. HIPAA's Security Rule specifies administrative, technical, and physical safeguards with which the covered healthcare entity must comply to assure the confidentiality of electronic protected health information.

The Social Security Act

The Social Security Act provides that "Social Security account numbers and related records that are obtained or maintained by authorized persons pursuant to any provision of law, enacted on or after October 1, 1990, shall be confidential, and that no authorized person shall disclose any such Social Security account number or related record" (42 U.S.C. § 405(c)(2)(C)(viii)). The Social Security Act also provides that "[w]hoever discloses, uses, or compels the disclosure of the social security number of any person in violation of the laws of the United States…shall be guilty of a felony…" (42 U.S.C. § 408(a)(8)).

The Privacy Act of 1974 (5 U.S.C. § 552a, note; P.L. 93-579, §§ 7(a) and 7(b))

The Privacy Act of 1974 provides that it is unlawful for any Federal, State or local government agency to deny any person a right, benefit, or privilege provided by law based on the individual's refusal to disclose his/her SSN, unless such disclosure was required to verify the individual's identity under a statute or regulation in effect before January 1, 1975, or such disclosure was required by Federal statute. Further, under *Section 7(b)*, a Federal, State or local government agency requesting that an individual disclose his/her SSN must inform the individual whether the disclosure is voluntary or mandatory, by what statutory or other authority the SSN is solicited, and what uses will be made of the SSN.

Scope and Methodology

To accomplish our objective, we

- visited 10 hospitals nationwide;
- interviewed hospital personnel responsible for patient admissions, information systems, medical records, and compliance with policy and procedures regarding the collection, use and protection of patients' Social Security numbers (SSN);
- reviewed applicable laws and regulations; and
- reviewed selected articles regarding hospital employees' and others' misuse of patient demographic data, including SSNs.

In addition, we visited the American Hospital Association and the American Health Information Management Association regarding hospitals' collection and use of SSNs. We also visited Blue Shield of California to discuss its experience of replacing SSNs with unique member identification numbers. We also contacted the Centers for Medicare and Medicaid Services regarding its use of SSNs as identifiers. The Social Security Administration entity reviewed was the Office of the Deputy Commissioner for Operations. We conducted our audit from May through September 2005 in accordance with generally accepted government auditing standards.

Hospitals Visited

Hospital	Location	Type of Control	Bed Size
University of Maryland Medical Center	Baltimore, MD	Nonprofit	726
Northwestern Memorial Hospital	Chicago, IL	Nonprofit	657
Brookwood Medical Center	Birmingham, AL	Profit	485
John H. Stroger, Jr. Hospital of Cook County	Chicago, IL	Government	459
Greater Baltimore Medical Center	Baltimore, MD	Nonprofit	314
Princeton Baptist	Birmingham, AL	Nonprofit	309
San Francisco General Hospital	San Francisco, CA	Government	303
Kaiser Permanente San Francisco Medical Center	San Francisco, CA	Nonprofit	243
Children's Hospital of Alabama	Birmingham, AL	Nonprofit	225
Cooper Green Hospital	Birmingham, AL	Government	148

Agency Comments

SOCIAL SECURITY

MEMORANDUM

Date: January 19, 2006 Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Inspector General

From: Larry W. Dye /s/
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report "Hospitals' Use and Protection of Social Security Numbers" (A-08-06-16056)--INFORMATION

We appreciate OIG's efforts in conducting this review. Our comments on the draft report content and recommendations are attached.

Please let me know if we can be of further assistance. Staff inquiries may be directed to Ms. Candace Skurnik, Director, Audit Management and Liaison Staff, at extension 54636.

Attachment:
SSA Response

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "HOSPITALS' USE AND PROTECTION OF SOCIAL SECURITY NUMBERS" (A-08-06-16056)

Thank you for the opportunity to review and comment on the draft report. We appreciate the report's acknowledgement that the Social Security Administration (SSA) cannot prohibit hospitals from using Social Security numbers (SSN) as patient identifiers and that the report also recognizes the challenges of educating hospital communities. Our responses to the specific recommendations are provided below.

Recommendation 1

SSA should coordinate with hospitals and relevant healthcare associations to educate hospitals about the potential risks associated with using SSNs as patient identifiers. For example, we believe the Agency should consider hosting or participating in conferences to discuss ways hospitals can enhance SSN integrity.

Response

We agree with the intent of the recommendation. While we can include information about the protection of the SSN as part of future presentations and conferences with medical providers where we are an active participant, our outreach efforts would be contingent upon the availability of resources. We will also consider using our Office of Disability Program's website, (http://co.ba.ssa.gov/disability/odp/professional_relations.html), as a resource for educating medical professionals about the potential risks associated with using SSNs as patient identifiers. This website is currently used to provide helpful information for the Professional/Medical Relations Officers and Regional Professional Relations Coordinators.

Recommendation 2

SSA should encourage hospitals to limit their collection and use of SSNs. For example, we believe hospitals should safeguard patients' SSNs by limiting access to hospital personnel and external entities with a business need to know and avoid displaying the entire number on any document, screen, or data collection field.

Response

We agree and will incorporate this recommendation in conjunction with existing and/or future outreach efforts as indicated in our response to recommendation 1.

Recommendation 3

SSA should encourage the Centers for Medicare and Medicaid Services (CMS) to remove SSNs from its identification cards and partner with them to develop an alternate identifier that meets both agencies' needs.

Response

We agree with the intent of this recommendation. On December 6, 2005, CMS advised us that they had conducted an internal survey in August 2005 to help them assess the impact of removing SSNs from Medicare cards. CMS is now finalizing a report of their findings. They intend to share their findings with SSA, the Railroad Retirement Board, and other governmental and nongovernmental third parties which would be impacted by any change involving the Medicare card and/or the use of alternative identifiers for Medicare/health insurance purposes. Any changes CMS is considering need to be evaluated in terms of the financial and systems impact the changes would have on the Agency. We look forward to reviewing CMS's report and working with them to ensure the SSN is protected from unnecessary and/or unauthorized disclosure.

Recommendation 4

SSA should promote the best practices of hospitals that are taking steps to limit their use of SSNs. For example, the Agency could promote best practices through activities, such as contributing articles to healthcare-related journals and association newsletters.

Response

We agree. Through our Office of Communications' partnerships with national and regional hospital associations, we will request that these organizations highlight best practices of hospitals who are taking steps to limit the use of the SSN in their healthcare-related magazines and newsletters.

OIG Contacts and Staff Acknowledgments

OIG Contacts

Kimberly A. Byrd, Director, 205-801-1605

Jeff Pounds, Audit Manager, 205-801-1606

Staff Acknowledgments

In addition to those named above:

Theresa Roberts, Senior Auditor

Kim Beauchamp, Writer-Editor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-08-06-16056.

DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Subcommittee on Human Resources

Chairman and Ranking Minority Member, Committee on Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Government Reform and Oversight

Chairman and Ranking Minority Member, Committee on Governmental Affairs

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

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

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Resource Management (ORM). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

Office of Audit

OA conducts and/or supervises financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

Office of Investigations

OI conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Finally, OCCIG administers the Civil Monetary Penalty program.

Office of Resource Management

ORM supports OIG by providing information resource management and systems security. ORM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, ORM is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.