Department of Veterans Affairs **VHA DIRECTIVE 2004-063**
Veterans Health Administration
Washington, DC 20420 **November 3, 2004**

OPERATING PROCEDURES FOR THE MANAGEMENT OF CENTERS FOR MEDICARE AND MEDICAID SERVICES DATA

1. PURPOSE: This Veterans Health Administration (VHA) Directive defines standard operating procedures (SOPs) for the management and distribution of the Centers for Medicare and Medicaid Services (CMS) data, in particular, CMS data that contain Individually Identifiable Health Information (IIHI), including, but not limited to, Social Security Numbers (SSNs), street addresses, and other identifiers.

2. BACKGROUND: VHA is committed to maintaining the integrity and security of veterans' health data in accordance with applicable laws and regulations. Compliance results in the organization being able to continue to use CMS data as a valuable information source. Non compliance results in the organization no longer having access to the data. ***NOTE:*** *Although all users of Medicare data will be held accountable for compliance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the Privacy Act, and other privacy statutes, as with all VHA data, ultimate compliance responsibility rests with VHA corporate officers.*

a. Operating procedures in this document have two objectives, to:

(1) Ensure compliance with the Standards for Privacy of Individually Identifiable Health Information, hence the HIPAA Privacy Rule, the Freedom of Information Act (FOIA), the Privacy Act of 1974, as well as Title 38 United States Code (U.S.C.) Section 5701 and Section 7332. ***NOTE:*** *Further information on applicable legislation can be found in Attachment A.*

(2) Facilitate the working together of disparate VHA components. VHA policy has shifted to implement the SOPs in an environment characterized by speed, simplicity, and cost effectiveness while demonstrating accountability and responsibility.

b. VHA uses IIHI to improve the clinical and financial performance of its health care system through both program administration and research analysis. Historically, VHA has attempted to balance the need to access health care information with the need to provide safe and high quality health care to veterans.

c. When data obtained from CMS contains any form of IIHI, VHA must comply with all applicable Federal privacy laws and regulations including FOIA, the HIPAA Privacy Rule, the Privacy Act, and 38 U.S.C. Section 5701 and Section 7332. CMS does not sell the data to VHA; however, as permitted under the Economy Act, CMS does charge VHA for administrative costs (e.g., processing, shipping, etc.) of processing the data.

d. The HIPAA Privacy Rule, Privacy Act, and other privacy statutes ensure the confidentiality of all IIHI used and disclosed by VA. For example, when an individual's IIHI is

included in a table, chart, exhibit, etc. the individual must remain anonymous. Information (e.g., SSN, street address, zip code, etc.) cannot be released without proper authority. Information with individual identifiers redacted out may be used and disclosed in a de-identified format without the restrictions applied by the privacy statutes.

e. IIHI is a subset of health information, including demographic information collected from an individual that:

(1) Is created or received by a health care provider, health plan, or health care clearinghouse;

(2) Is related to the past, present, or future condition of an individual, and the provision of, or for, payment for health care; and

(3) Identifies the individual, or provides a reasonable basis to believe the information can be used to identify the individual.

3. POLICY: It is VHA policy to establish a central order and/or distribution point for CMS data which will be the only recipient for CMS data. ***NOTE:*** *This is consistent with the CMS requirement that VHA have only one recipient for CMS data, and it reduces the likelihood of duplicate, expensive data being ordered from CMS.*

4. ACTION

a. **Primary Recipient.** The Medicare and Medicaid Analysis Center (MAC) in Braintree, MA, have been designated as the Primary Recipient of Medicare Data for VHA. MAC is a field office of the Assistant Deputy Under Secretary for Health. The Assistant Deputy Under Secretary for Health pays CMS to provide all data to VHA. As the Primary Recipient, MAC is responsible for:

(1) Ordering data from CMS based on requests from Secondary Recipients.

(2) Distributing data as requested to Secondary Recipients, using the most secure methods consistent with overall policy.

(3) Maintaining records of ordered and distributed data and, where applicable, associated SSNs for each year of data.

(4) Working with VA Information Resource Center (VIReC) and others, to create a finder file of Veteran SSNs available from within the VHA to provide CMS by June 1 of each year. CMS, in turn, will merge these SSNs with all SSNs within the Medicare system. Patient utilization files for all VA-Medicare matches along with other purchased data will be returned to MAC.

(5) Ordering CMS files twice yearly. The majority of CMS data is ordered on June 30, just prior to the expected July availability date. Requests for CMS data must be made to MAC by June 15 to be ordered by June 30. MAC orders additional CMS data on December 31 for

requests received by December 15. On May 1 and November 1, the responsible individual at MAC informs Secondary Users of impending order and important dates.

(6) Ensuring the safety of computer systems and data tapes by keeping them in locked facilities and by utilizing appropriate security protocols (see VA Handbook 6210).

(7) Establishing a Contingency Plan to ensure data recovery within a minimum of a 1 to 2-week period.

(8) Exploring the feasibility of utilizing the Austin Data Processing Center as a repository for all CMS data in the case of catastrophic failure of servers at the MAC or secondary user sites.

(9) Providing programming support to ensure the year-to-year compatibility of CMS data.

(10) Maintaining a record of names and addresses of responsible individuals at Secondary Recipient sites (e.g., VA Information Resource Center (VIReC) and Assistant Deputy Under Secretary for Health).

(11) Developing, with direction from the Oversight Team (see subpar. 4f), the Data Use Agreement (DUA) between VHA and CMS

(12) Serving as the official repository for the VHA-CMS Memorandum of Understanding (MOU), Federal Register, System of Records and Operating Procedures, and other documents pertaining to CMS.

(13) Ensuring the required documentation (see Att. C).

b. **Secondary Recipients**

(1) Secondary Recipients serve as research and analytical centers. In addition, they store, distribute, and maintain CMS data received from MAC. Secondary Recipients are required to provide the Assistant Deputy Under Secretary for Health with 3-year forecasts of CMS data they plan to request in order to enable the Office of the Assistant Deputy Under Secretary for Health to more efficiently build these new files into its budgeting process. ***NOTE:*** *Current CMS data included in the Assistant Deputy Under Secretary for Health's budget and the new CMS data requested in June 2004, are in Attachment B.* Current Secondary Recipients are:

(a) Assistant Deputy Under Secretary for Health. The Assistant Deputy Under Secretary for Health, located in Washington, DC, conducts analysis in support of the Under Secretary for Health, Deputy Under Secretary for Health, and Veterans Integrated Services Network (VISN) Directors. The Assistant Deputy Under Secretary for Health staff receives CMS data tape cartridges from MAC, and has a server dedicated to their use. The Assistant Deputy Under Secretary for Health Statistical Analysis System (SAS) programmers using the server have been provided access to CMS data and non-SAS programmers have been provided access to tables that summarize the data.

(b) VA Information Resource Center (VIReC), Hines VA Hospital, Hines, IL. VIReC manages and distributes VA-Medicare linked data files to VA researchers as part of the VA-Medicare Data Merge Initiative. Because of the intricate nature of research regulation, all requests for Medicare data for research purposes must be made through VIReC. VIReC has established standard procedures for acquiring, processing, and releasing Medicare data to researchers that comply with all HIPAA, Privacy and 38 U.S.C. requirements mentioned previously, and take into account the special regulatory provisions for research.

(c) Patient Care Services (PCS). PCS conducts analysis in support of the Under Secretary for Health and the Deputy Under Secretary for Health. PCS staff have dedicated mainframe capacity at the Austin Data Processing Center (DPC) and receive CMS data on CDROM media or tape from MAC. PCS SAS programmers using the mainframe are provided access to CMS data, and non-SAS programmers are provided access to tables that summarize the data.

(d) The VISN Support Service Center (VSSC). The VSSC is a health care information and technical support organization serving both the needs of the Deputy Under Secretary for Health for Operations and Management(10N) and the individual VISNs.

1. The VSSC supports field operations in the areas of Information Management; Capital Programs; Capital Asset Realignment for Enhanced Services (CARES); National Veterans Service and Advocacy Program (NVSAP); and, Planning and Data Analysis.

2. The Management Science Group (MSG) is now part of the VSSC.

3. The VSSC also provides support for special projects and initiatives at the request of the Deputy Under Secretary for Health for Operations and Management(10N), VISNs, and the National Leadership Board.

4. The VSSC computer systems operate entirely within the VA network and access to the computer system is limited to the VA network. System access is limited to only those authorized VSSC staff members. ***NOTE:*** *Data owners for VSSC are the Director, VSSC and the Director, MSG.*

(2) Secondary Recipients must submit a plan to the Oversight Team for approval before they may distribute data to individual users. The plan must state the Secondary Recipient's proposed distribution to users and their strategy for securing data and ensuring compliance with privacy statutes. Upon approval by the Oversight Team, this plan serves as a binding agreement of operation between the Primary Recipient and the Secondary Recipient. In addition, Secondary Recipients must:

(a) Maintain a list of names, telephone numbers, addresses of all Individual Users (including contractors) to whom they have given access to CMS data, as well as their dates of use.

(b) Maintain confidentiality and non-disclosure agreements for all Individual Users given access to CMS data.

(c) Safeguard the security of CMS data through strict administrative and technical standards. At the technical level, VHA maintains a protected environment by using measures such as user-specific database access privileges, internal and external user authentication, secure and encryption techniques, and active intrusion detection.

(d) Ensure compliance with VHA privacy directives and data security handbooks, including assignment of individually unique user identification codes and individually unique passwords.

(e) Develop a Contingency Plan that ensures data recovery within 1 to 2 weeks.

(f) Periodically review cell sizes being reported, and communicate cell size standards to the Oversight Team and Individual Users. ***NOTE:*** *Currently, cell sizes of 11 or greater are acceptable while cell sizes of 10 or fewer are unacceptable.*

(g) Communicate to Oversight Team and Individual Users the policy on retention and disposition of CMS data. Data needs to be destroyed after 10 years, unless selected series require retention for a greater period of time.

(h) Develop a Business Associate-Trading Partner Agreement, if applicable, between contractors and the Secondary Recipient specifying responsibility for:

1. Cyber security,

2. Allowable analytical cell size,

3. Controlling access to the data, and

4. End of contract requirements to destroy the data.

(i) Train new and current employees about the computer system, including:

1. Data and information security standards, procedures, and requirements; and

2. Structure, content, strengths, weaknesses and applications of the CMS datasets and their applicability to VA data comparisons.

(j) Confer periodically with Individual Users to:

1. Review fundamentals of, and changes in, compliance with HIPAA and Privacy laws; and

2. Discuss changes in security or operating procedures.

(k) Transmit IIHI using passwords and/or appropriate encryption techniques, or by a courier service that provides ground tracking of packages they deliver. There will be no electronic transfer of IIHI via the Internet, e-mail, or file transfer protocols (FTP).

(l) Successfully pass audits of security infrastructure and compliance with regulations associated with HIPAA, the Computer Security Act, and the Federal Information Security Management Act (FISMA).

c. **Individual Users.** Individual Users can be VA or VHA employees, contractors with whom VA has developed business associate agreements, or affiliated university faculty with VA appointments. They may use scrambled SSN data for research or management purposes. Data may be transferred off site to authorized faculty or contractor offices; however, data cannot be transferred to non-VA entities. Every individual user who requests Medicare data is required to:

(1) Sign and abide by the following privacy statement:

"PRIVACY STATEMENT: It is the policy of VHA to protect the patient's rights of confidentiality. The requestor, in exchange for receipt of patient level data, agrees to use the data only as described and for the purpose(s) stated in this request. The data custodian further agrees to provide a secure environment for storage and use of the data and any working files to prevent unauthorized access. The requestor will comply with all Privacy Act and HIPAA Privacy Rules."

(2) Comply with VA data security, data privacy, data base utilization, and, for researchers, Human Subject Protection training requirements.

(3) Follow the VHA privacy directives in Handbook 1605.1 and have signed an Access Notice (Rules of Behavior), as required by VHA Directive 6210 and OMB Circular No. A-130 (Rules of the System).

(4) Prevent re-identification of an individual's protected health information from published or otherwise disseminated tables and charts containing potentially identifiable data. Prevention of re-identification is traditionally ensured by limiting the cell size in tables and charts depending on the type of data included.

d. **Assistant Deputy Under Secretary for Health.** The Assistant Deputy Under Secretary for Health, or designee, is responsible for designating an Oversight Team to review and ensure system security and compliance with all policies and regulations regarding use of the data (e.g., authority to maintain the data, routine use, data security such as safeguards, data storage, retrievability, retention and disposal; privacy including notification procedures and records access procedures).

e. **Oversight Team**

(1) Annually the Oversight Team must submit a letter to the Assistant Deputy Under Secretary for Health indicating the status of VA regarding compliance with all applicable polices and regulations. If necessary, the letter needs to indicate concerns or deficiencies and steps being taken to eliminate them.

(2) In addition the Oversight Team is responsible for:

(a) Providing leadership.

(b) Establishing overall direction and broad operating procedures, having the characteristics of speed, simplicity, and cost effectiveness.

(c) Ensuring management responsibility and accountability.

(d) Updating and monitoring operating procedures.

(e) Communicating operating procedures and plans within VHA, and to VA, as needed.

(f) Promoting the use of CMS data.

(g) Reviewing and recommending establishment of "Secondary Recipient" sites.

(h) Conferring with Assistant Deputy Under Secretary for Health on systems upgrades and costs at MAC, to ensure cyber security.

(3) The Oversight Team consists of core and advisory members. Core members are the decision-making group and represent Primary and Secondary Recipients, as well as VHA management as indicated on the VHA-CMS MOU. Advisory members produce audits, provide updates, and since there is overlap in these areas, the auditors will be required to plan and coordinate audit activities. Advisory members are represented by:

AUDITORS	**FOCUS OF AUDIT**
VHA HIPAA Program Management Office	HIPAA
VA Office of Cyber and Information Security	Cyber Security
VHA Privacy Office	Privacy Act, Title 38 United States Code, 5701 and 7332
VHA Office of Information Technology	Need for additional systems capacity and efficient use of existing systems.

(4) The Oversight Team meets periodically, but at least two times per year to:

(a) Review annual audits of VHA's security infrastructure related to the CMS data, receive updates on new approaches to cyber security from the Office of Cyber and Information Security, and make decisions for appropriate changes to operating procedures.

(b) Review annual audits of VHA's compliance with HIPAA, Privacy Act, and other privacy statutes; receive updates from HIPAA and Privacy officials about new interpretations or changes in HIPAA and Privacy laws and their implications; and to make decisions for appropriate changes to operating procedures.

(c) Review Secondary Recipient policy on analytical cell size, retention, and disposition of data. ***NOTE:*** *Since Secondary Recipients have unique missions and serve unique customers, they are individually responsible for establishing policies in these areas.*

(d) Facilitate the development of Operating Procedures at new Secondary Recipient sites.

(e) Develop strategy to promote the use and communicate the availability of CMS data.

(f) Review finder file procedures and standard files requested from CMS.

5. REFERENCES

a. Title 38 CFR 1.550-557, Freedom of Information Act (FOIA).

b. Title 5 U.S.C. 552a, Privacy Act of 1974.

c. Title 38 CFR 1.575-582, Privacy Act of 1974.

d. Public Law 104-191, Health Insurance Portability and Accountability Act (HIPAA) of 1996.

e. Title 45 CFR Parts 160-164, Standards for Privacy of Individually-identifiable Health Information.

f. OMB Circular A-130. Management of Federal Information Resources, Appendix I Federal Agency Responsibilities for Maintaining Records About Individuals.

g. Title 38 U.S.C. 5701, Confidential Nature of Claims.

h. Title 38 U.S.C. 7332, Confidentiality of Certain Medical Records.

i. Title 38 CFR 1.460-496, Confidentiality of Certain Medical Records.

j. VHA Handbook 1605.1, Privacy and Release of Information.

k. VA Directive 6210, Automated Information Systems (AIS) Security Procedures.

6. FOLLOW-UP RESPONSIBILITY: The Office of the Assistant Deputy Under Secretary for Health is responsible for the contents of this Directive. Questions are referred to 781-849-1837, extension 200.

7. RECISSIONS: None. This VHA Directive expires November 30, 2009.

S/Jonathan B. Perlin, MD, PhD, MSHA, FACP
Acting Under Secretary for Health

DISTRIBUTION: CO: E-mailed 11/04/04
FLD: VISN, MA, DO, OC, OCRO, and 200 – E-mailed 11/04/04

ATTACHMENT A

NOTES ON PRIVACY LEGISLATION

1. HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

a. The purpose of HIPAA is "To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes." There are five sections (i.e., Titles) to this legislation.

(1) Title I of HIPAA, Health Care Access, Portability, and Renewability, protects health insurance coverage for workers and their families when they change or lose their jobs.

(2) Title II includes Fraud and Abuse Medical Liability Reform and Administrative Simplification provisions.

(3) Title III addresses Tax Related Health Provisions.

(4) Title IV addresses Group Health Plan Requirements.

(5) Title V outlines Revenue Off-Set provisions.

b. The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data. Adopting these standards improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care.

c. The legislation establishes requirements for:

(1) Electronically conducted health care transactions;

(2) Use and disclosure of protected health information;

(3) Security of electronic protected health information (EPHI);

(4) Information storage, access, physical protection; and

(5) Contingency planning and disaster recovery.

d. Administrative Simplification requirements set forth standards for identification enumeration of payers, providers, employers, and patients.

2. PRIVACY ACT

a. The purpose of the Privacy Act of 1974, Title 5 United States Code § 552a (2000), is to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from Federal agencies' collection, maintenance, use, and disclosure of personal information about them.

b. The Act focuses on four basic policy objectives:

(1) To restrict disclosure of personally identifiable records maintained by Federal agencies;

(2) To grant individuals increased rights of access to Federal agency records maintained on themselves;

(3) To grant individuals the right to seek amendment of Federal agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely or complete; and

(4) To establish a code of "fair information practices" that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

c. In order to meet the legislation requirements imparted by the Act, government agencies must:

(1) Establish policies regarding the collection and maintenance of records,

(2) Publish a notice regarding the existence and character of all systems of records, and

(3) Maintain an accounting of disclosures.

ATTACHMENT B

DATA FILES ORDERED OR AT THE MEDICARE AND MEDICAID ANALYSIS CENTER (MAC)

FILE	YEAR(S)
1. Stay Level	
Medicare Provider Analysis and Review (MEDPAR) – Inpatient	1999-2003
2. Standard Analytical Files (SAF)	
Part A	
Inpatient SAF	2003
Skilled Nursing Facility	1999-2003
Outpatient	1999-2003
Home Health Agency	1999-2003
Hospice	1999-2003
Part B	
Physician and/or Supplier (Carrier)	1999-2003
Durable Medical Equipment	1999-2003
End Stage Renal Disease (ESRD) Patients	
United States Renal Data System (USRDS) SAF with cross-reference of VHA SSN cohort	2003
3. Patient Enrollment Files	
Denominator	1999-2003
4. Patient Identification Files	
SSN-Health Insurance Claim (HIC) Conversion or equivalent	2003
HIC Cross-reference or equivalent	2003
Vital Status	1999-2003

5. Other Files

Uniform Provider Identification Number (UPIN)	2003
Group Health Plan	1999-2003
Provider of Service	1999-2003
Medicare Current Beneficiary Survey (MCBS) with cross-reference of VHA SSN cohort	2003
Denominator (100 percent) with cross-reference of VHA SSN cohort	2003

ATTACHMENT C

REQUIRED DOCUMENTATION

In order to acquire and continue to use Centers for Medicare and Medicaid Services (CMS) data, a set of documents describing the legal, contractual and management components of the CMS relationship must be maintained. This responsibility has been delegated to the Medicare and Medicaid Analysis Center (MAC). In addition, regulations require that the nature of the obtained data, its use, and the systems established to ensure Veterans Health Administration (VHA) compliance with rules and regulations be recorded and easily accessible. Documents required to be maintained are:

1. Memorandum of Understanding (MOU). An MOU is an agreement between the VHA and CMS describing the CMS-VHA relationship and identifying the responsible VHA person for communicating, managing, and monitoring the relationship.

2. Data Use Agreement (DUA). A DUA is an agreement between the Primary Recipient and CMS defining what data will be used and for what purposes.

3. Federal Register Announcement. This is a public announcement stating VA's intention to develop a System of Records (SOR) using Individually Identifiable Health Information (IIHI). The announcement defines the SOR and its uses, identifies data users, and provides the name, location, and management of the SOR. In addition, the Federal Register announcement provides the public with an opportunity to comment on Agency planned actions.

4. One-time Responses to Questions from the CMS Privacy Board. This is a one time document reviewed by the CMS Privacy Board prior to releasing ordered data.

5. Operating Procedures. Recent interpretations by CMS of the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the Privacy Act have resulted in VHA assuming more responsibility for compliance with the HIPAA Privacy Rule and the Privacy Act for IIHI disclosed to VHA. Operating procedures are required to ensure compliance by all VHA users of CMS data. ***NOTE:*** *This Directive fulfills this requirement.*