PROGRAM MEMORANDUM INTERMEDIARIES/CARRIERS

Department of Health and Human Services

Health Care Financing Administration

Transmittal No. AB-01-11 **Date JANUARY 26, 2001**

CHANGE REQUEST 1439

HCFA has revised its information technology (IT) security requirements for Medicare carriers, intermediaries, DME regional carriers, their data centers, standard system maintainers, and program safeguard contractors. The requirements may be found in the HCFA Business Partner Systems Security Manual. The purpose of this Program Memorandum (PM) is to provide supplemental instruction on how and when HCFA expects the new requirements to be implemented.

Overview

HCFA is launching a multi-year initiative to improve the management of information systems security for each of it Medicare contractors. The initiative has four key objectives:

- Establish baseline (core) security requirements;
- Assess Medicare contractor compliance with baseline;
- Fund Medicare contractor compliance efforts; and
- Evaluate contractor security performance.

In FY 2001, HCFA is implementing these objectives through: 1) New and revised security requirements in the Medicare Carriers and Intermediary Manuals, 2) FY 2001 productivity investment funds to implement the new requirements, 3) Review of security program documentation by HCFA's independent verification and validation contractor, and 4) Development of future security funding requirements from Medicare contractors' documentation of their accomplishments, gaps and estimates of future funding requirements.

Implementation and Funding

The HCFA Business Partners Systems Security Manual contains new or expanded instructions that require contractors to develop and implement information technology security policies, procedures, plans and controls. These new instructions are in addition to previous, and substantially unchanged, security requirements that contractors have been in the carrier and intermediary manuals for many years and which are covered in the regular operating budget. These existing requirements include an annual compliance audit, a triennial risk assessment; and contingency plan development and testing.

In FY 2001, HCFA will provide productivity investment funds to contractors for the management analysis and planning tasks necessary to:

- Assess compliance with the HCFA core security requirements;
- Comply with the new or expanded security controls contained in the core requirements;
- Develop a security architecture for system-specific IT systems security plans and;
- Prepare and submit documentation, gap analysis and funding requirements to HCFA.

The productivity investment funds will be automatically distributed to you. The funding allocation was based on providing approximately one full time equivalent to each Medicare contractor. Where it was seen that a contractor was running multiple systems, the contractor will only be provided with

the base funding amount in an effort to eliminate duplicate funding. Medicare contractors that are Technical Advisory Group members will be provided additional funding as they have agreed to provide additional assistance to HCFA to "Fast Track" certain activities. Verizon will not be required to perform the tasks above since they will be transitioning out of the Medicare program within the near future.

HCFA expects Medicare contractors to continue to fund longstanding and continuing security requirements like staffing a security officer, conducting annual compliance audits, conducting risk assessments and, preparing and testing contingency plans through your regular Medicare operating budget. You may find these requirements in the program management section of your FY 01 budget and performance requirements.

HCFA Core Security Requirements Assessment

HCFA will provide every Medicare contractor with a tool to use in assessing, documenting and reporting on your compliance with HCFA core security requirements. The use of this tool, referred to as the Contractor Assessment Security Tool (CAST), is mandatory. Detailed instructions for acquiring, installing and securing technical assistance on CAST are provided at: www.HCFA.gov/EXTPART.

Contractors must submit their security program documentation to HCFA by **July 31, 2001**. The documentation will consist of a CAST-generated report and selected supporting documentation. HCFA has two uses for this report. First, it will be used to assess the gap between your actual security program and HCFA core requirements. This information, when combined with the funding requirement information (discussed below), will be used to develop contractor security budget performance requirements for FY 2002 and subsequent years. Second, HCFA's independent verification and validation contractor will review the report and its supporting documentation. They will determine if all the core requirements have been met and assess the technical approach used to satisfy them. Their findings may be included in the FY 2001 contractor performance evaluation.

Annual Compliance Audit

Section 2974D of the Intermediary Manual and §5137D of the Carriers Manual require you to conduct an annual compliance audit of your systems security program. These sections are being replaced by §3.5 of the Business Partner Systems Security Manual that continues the annual compliance audit requirement. The new manual states that you must focus the audit on 4 categories of the core security requirements specified in advance by HCFA. The 4 categories that must be audited in FY 01 are: Access Control; Segregation of Duties; Service Continuity and; Application Software Development and Change Control.

Security Plans

The revised Carriers and Intermediary Manuals contain a new requirement - Medicare contractors must develop security plans for their general support systems (GSS) and each major application (MA). The plans must cover all of the systems that are mission-critical to your Medicare line of business-these include your data center(s), LANs, WANs, and major applications (claims processing and your "front-end and back-end applications" for example, EDI gateway, printing, and financial applications).

Security plans are relatively complex and have many interdependencies (such as your standard system and CWF maintainers, data center operator(s), etc.) In view of limited IT systems security funding, you are not required to develop core-security requirement compliant security plans for each of you GSSs and MAs in FY 01. Medicare contractors should, instead, develop a security plan architecture. You should review the core security requirements for system security plans and begin determining which of your systems will require security plans and estimate the level of effort required to produce them. In the event that you already have system-specific security plans that satisfy HCFA core requirements, you will not need to develop new ones. You should, however, prepare a crosswalk to facilitate compliance assessments. HCFA will work with the standard system

maintainers (claims processing, CWF and its claims processing data center) to develop IT systems security plans that may be incorporated into your security plan architecture. Your security plan architecture report, including identification of GSSs or MAs for which compliant security plans already exist, must also be submitted by **July 31, 2001**.

Gap Analysis and Future Funding

In order to continue supporting Medicare contractor security efforts in future fiscal years, HCFA will need information from you. We will ask you to estimate the cost of:

1. Implementing unmet core security requirements;
2. Developing system-specific security plans; and
3. Security engineering.

- You will be asked to indicate which of these IT systems security requirements, plans or engineering future funding needs are specific to Medicare and which are corporate-wide.
- You will be required to provide information on the basis of the Medicare share of your cost estimates.
- You should not request security engineering funds for a system unless there is a security plan for that system which shows unmitigated risks.

This information must be reported to HCFA by **July 31, 2001.**

Follow-on Program Memorandum (PM)

HCFA will issue another PM in the February/March 2001 timeframe which will provide supplemental instructions on how, when, and where to submit the following:

1. Core security requirement assessment report and supporting documentation;
2. Security plan architecture report; and
3. Gap analysis and funding requirements report.

Internet Policy

Health care transactions (claims, remittances, etc.) are prohibited between Medicare carriers/ intermediaries and providers over the Internet. This Internet prohibition also applies to using the Internet to transport HCFA Privacy Act-protected data between carriers/intermediaries and any other party. (See http://www.hcfa.gov/security/isecplcy.htm for a definition of protected data.) HCFA is closely following the health care industry's movement toward adoption of industry-wide security technologies that assure confidentiality, integrity and availability of data moved over the Internet and will reconsider its policy at the appropriate time.

Summary of Key Dates

Conduct core security requirements self-assessment.	July 31, 2001
Submit Security Program Documentation to HCFA	July 31, 2001
Submit Security Plan Architecture Report	July 31, 2001
Submit Information Systems Security Funding Requirements to HCFA	July 31, 2001
Conduct Annual Compliance Audit	No later than September 30, 2001
Conduct Triennial Risk Assessment	No later than September 30, 2001
Update Contingency Plan and Test	No later than September 30, 2001

Security Questions and Concerns

HCFA expects that you may have questions or concerns about the new security requirements in the manual, CAST or this PM. You may send them to: Security@HCFA.gov. We will provide a prompt direct response as well as posting it to a Frequently Asked Questions (FAQ) page on the HCFA Medicare Contractor Information Systems Security web site. Its address is: www.HCFA.gov/EXTPART.

The effective date for this PM is January 26, 2001.

The implementation date for this PM is January 26, 2001.

This PM may be discarded January 26, 2002.