Program Memorandum Intermediaries

Department of Health and Human Services (DHHS)
Centers for Medicare and Medicaid Services (CMS)

Transmittal A-01-85 **Date: JULY 19, 2001**

CHANGE REQUEST 1749

SUBJECT: Notification of Access to Eligibility Vendors

This Program Memorandum (PM) is to clarify instructions in Transmittal Number 1803, dated August 3, 2000, (Change Request 1231) Medicare Intermediary Manual, Part 3, Claims Process; and Transmittal Number AB-01-11, dated January 26, 2001 (Change Request 1439), Information Technology (IT) Security Requirements for Medicare contractors. You should communicate the information in this PM to all current eligibility vendors, as well as to any new vendors.

Granting Access to Eligibility Data

Based on recent contacts and discussions between Medicare contractors and certain eligibility vendors, we want to clarify the roles and responsibilities of our Medicare contractors regarding the granting of access to eligibility data. Medicare data is privacy protected and is available to providers to ensure the accurate submission of Medicare claims. It is not available for storage for subsequent utilization, e.g., marketing.

In addition to following the instructions contained in the references above, Medicare contractors are to emphasize to vendors, who seek access to eligibility data on behalf of providers, that:

1. The network service agreement that the vendor signed prohibits them from storing data for any longer than required to ensure the data have reached their destination, (That is, data is stored solely for the purpose of retransmission in case of error in the original transmission and is erased upon confirmation of successful transmission.)
2. The adherence to security and privacy requirements to preserve the integrity of this sensitive data is of paramount importance, and
3. Any failure to abide by these requirements will result in termination of access.

Systems Security Requirements

An additional restriction on the granting of access to eligibility data is CMS's Internet Policy. CMS's Program Memorandum (PM) for intermediaries and carriers, Transmittal Number AB-01-11 dated January 26, 2001, affirmed the policy. The PM states in part, "Health care transactions (claims, remittances, etc.) are prohibited between Medicare carriers/intermediaries and providers over the Internet. The Internet prohibition also applies to using the Internet to transport CMS Privacy Act protected data between carriers/intermediaries and any other party."

This prohibition practically means that we require the use of private network or a dial-up connection between any vendor and the Medicare contractor for the electronic transmission of all health care transactions and Privacy Act protected data.

CMS policy, however, does allow Privacy Act protected data to be transmitted between providers and other parties who are <u>not</u> Medicare contractors over the Internet if it is authenticated and encrypted. CMS policy does require organizations desiring to use the Internet to notify CMS of their intent. CMS reserves the right, as noted in the policy, to both require the submission of documentation to demonstrate compliance with requirements or to conduct on-site audits, if necessary, to ascertain compliance. Auditable documentation includes systems security plans and

policies relating to the Internet connectivity. Audits may include ethical penetration tests at the vendor and/or the Medicare contractor to ensure the private line connection established to protect Medicare data can not be compromised in any way by communication links between the vendor and its provider base.

Advising Your Providers and Network Service Vendors

Vendors should be given some guidelines to prepare their customers to use sensitive beneficiary-related data. We require that logon requests made on behalf of their customers be confined to personnel on a need-to-know basis. This should be reserved to a limited number of staff in the patient intake and accounts resolution areas of the customers' operations. These personnel should be trained in the proper handling of the sensitive data, and appropriate security procedures enforced, e.g., unique user IDs and passwords for each individual and desktop/server security measures separating the private line connections from other desktop functionality such as the Internet. Customer service material should be developed and implemented for all personnel using or with access to the sensitive beneficiary-related data.

Questions and Concerns

Questions on the eligibility claims process requirements should be addressed to Jean Gross, by e-mail (Jgross3@cms.hhs.gov) or phone on (410) 786-6159, or Gladys Wheeler, by e-mail (Gwheeler@cms.hhs.gov) or phone (410) 786-0273). Questions on the security requirements should be directed to Security@cms.hhs.gov.

We will provide a prompt response to questions received, as well as posting the answers to our EDI (www.hcfa.gov/medicare/edi/edi.htm) or Security (www.hcfa.gov/extpart) websites.

The *effective date* for this PM is July 19, 2001.

The *implementation date* for this PM is July 19, 2001.

These instructions should be implemented within your current operating budget.

This PM may be discarded after June 30, 2002.