Medicare Claims Processing Manual

Chapter 31 - ANSI X12N Formats Other than Claims or Remittance

Table of Contents

(Rev. 96, 2-6-04)

Crosswalk to Old Manuals

1 - Purpose of Chapter

(Rev. 1, 10-01-03)

This chapter contains instructions for implementation and processing formats

- ANSI X12N 270/271 (Inquiry and Response);
- ANSI X12N 276/277 (Claims Status Request and Response; and
- ANSI X12N 278 (Electronic Referral Certification and Authorization

In general these will be formats accepted by intermediaries and carriers, including RHHIs and DMERCs

10 - ANSI X12N 270/271 Implementation and Direct Date Entry (DDE) Eligibility

(Rev. 1, 10-01-03)

PM AB-03-036

10.1 - Background

(Rev. 1, 10-01-03)

This section provides instructions for implementation of format ANSI X12N 270/271, version 4010A1, under the Health Insurance Portability and Accountability Act (HIPAA) It applies to Intermediaries, Carriers, Durable Medical Equipment Regional Carriers (DMERCs), herein referred to as “contractors,” It also applies to Data Centers (DCs), their respective shared systems maintainers, and the Common Working File (CWF) maintainer.

10.2 - Eligibility Queries Options and Workflow

(Rev. 1, 10-01-03)

The following provides a basic description of the process to be followed. In addition to the workflow shown in this subsection supplemental information explaining requirements listed in the workflow is shown in §10.8. The role of the various parties involved in the process is also shown in later subsections.

Unlike other Electronic Data Interchange (EDI) transactions implemented by Medicare, electronic eligibility queries will by-pass contractor front and back ends and will be routed to the appropriate CWF Customer Information Control System (CICS) region via a connection to the Medicare Data Center Network (MDCN) through the appropriate data center.

Although much of the workflow below refers to IVANS connectivity, DDE connections are to continue where the capability currently exists. Private network and LU6.2 connections for eligibility data established by individual contractors can continue to be supported where the capability currently exists at the contractors discretion, but must also be routed to the appropriate CICS region through the MDCN and the data center. Private network and LU6.2 connection 270 queries are subject to the same CWF security verification and error reporting as indicated below for IVANS connections.

DDE connections are also subject to rejection if unable to obtain authorization from the CWF security module (described below). All eligibility queries will be processed in real-time. Medicare will not accept batch eligibility queries or issue responses in batch.

1. The contractor must:

    a. Notify their providers and network service vendors of their eligibility options and of when the contractor is to be notified of changes that may impact their connection for receipt of eligibility data;

    b. Determine if any current LU 6.2 and private network connections used to furnish eligibility data electronically will continue to be supported;

    c. Submit a funding request to their Consortium Contractor Management Specialist (CCMS) HIPAA representative, with a copy to their regional financial management contact, within three weeks of the issue date of this PM for incremental costs related to implementation and FY 2003 operation of this eligibility inquiry process. This funding request must separately itemize incremental costs for:

        i. Assessed share of data center costs;

        ii. Submitter testing costs if not already submitted to CMS for HIPAA testing in general for FY 2003; and

        iii. Other costs (itemize the “other” costs and identify the cost for each itemized activity).

    d. Coordinate procedures for interaction with and for reporting of IP address and port changes with their data center.

2. The provider must decide whether to:

a. Continue to use DDE access to obtain eligibility data, where that functionality is furnished by their contractor. A CWF module operating at each data center will generate the screen eligibility data to be viewed via DDE. DDE will begin to report some additional eligibility data such as managed care coverage;

b. Continue to use LU 6.2 connection, where it will continue to be supported, to obtain 271 data;

c. Continue to use a private network connection, where it will continue to be supported, to connect to a data center to obtain 271 data;

d. Establish a direct connection with the data center via IVANS for use of the 270/271; or

e. Contract with a network service vendor that will channel eligibility data requests to/from the data center on behalf of the provider.

Whether the provider continues with a current connection methodology or changes to another connection methodology, the provider must notify the contractor of changes that would impact the information entered in the CWF security module.

3. If the provider decides to contract with a network service vendor, the provider must:

    a. Sign an agreement with the network service vendor, that includes security and privacy specifications for the data, obtain passwords and ID numbers from that vendor for provider staff authorized to obtain the information, pay costs as assessed by the vendor, and load software from the vendor to establish that connection;

    b. Furnish the Medicare contractor with a signed statement authorizing the network service vendor to act as their agent to obtain eligibility data, sign a Medicare Electronic Data Interchange (EDI) agreement with the contractor if not previously done, and agree to notify the contractor of any change in vendor or if they cease to use a vendor to obtain eligibility data. In the event the provider will not also submit claims electronically, the EDI agreement must be modified to exclude language specific to claims or to transactions other than eligibility queries.

4. The network service vendor must contact the contractor to sign a network service agreement.

5. If a provider decides to directly connect through IVANS, the provider must notify the contractor of their intent.

6. The contractor must:

a. Sign a sponsorship agreement (which can be signed by a Medicare EDI supervisor or higher individual at the contractor) with IVANS agreeing to pre-clear all providers and network service vendors referred to IVANS for connectivity for eligibility data (contractors are to contact rex.bevis@ivans.com or phone 513-271-5668 if not yet contacted by IVANS concerning the sponsorship agreement);

b. Determine whether the provider and/or network service vendor should be allowed to connect to the data center to obtain eligibility data. Use the same criteria that would previously have been used to determine whether a provider or network service vendor should have been given access to the eligibility data through contractor's own front end;

c. Notify IVANS of the contact information for an approved provider/network service vendor;

d. Populate the provider's/network service vendor's information into the CWF security module (see the CWF specifications located on the following Web site: http://cms.csc.com/cwf/) that resides at the data center, and request a user ID and password from the data center for the pertinent CICS region(s). Where a port number is also needed for further identification, that number will need to be identified as part of the client address as MDCN cannot read port numbers in a network layer. The contractor must furnish the user ID and password to the provider, or the provider's designated network service vendor. The user ID is for the use of the 270 submitter, either the provider or the network service vendor as applicable;

   i. The contractor must also populate the CWF security module with information for those providers/vendors that will continue to use LU6.2, a private network, or DDE to access the CWF eligibility module, and update that file to reflect changes as needed.

   ii. The contractor must make any needed changes to their supported private network and LU6.2 connections that may be needed to enable interaction through the MDCN with the CWF modules residing at the data center.

   iii. The contractor must notify their private network and LU6.2 customers of any differences they will encounter in error messages received as result in this change in the source of the eligibility data.

e. Forward the IP address and port number as part of the client address where applicable for connection to the CICS region to IVANS (a vendor would be issued a separate IP address for each data center and a unique port number for each CICS region it is authorized to access);

f. Furnish the provider or vendor with information on:

i. The proprietary messages that could be generated by CWF due to failure of the transaction to meet the implementation guide semantic requirements;

ii. Situations when a TA1 would be issued and a description of the TA1 error codes, e.g., 006, that could be issued;

iii. Situations when a 997 would be issued to report syntax errors in the transaction;

iv. Situations when a 271 would be returned with error information, e.g., code 42 in AAA03 and an error code and message in the prefix;

v. Action to be taken by the provider/vendor if any of the error messages are received.

vi. Notify vendors/providers how to connect to the ELGA or ELGB screens to obtain eligibility information, if applicable.

vii. Notify vendors/providers of the CWF Host Site ID, which must be inserted in ISA08 of the 270 transaction. The ISA07 must include the "ZZ" qualifier. Contractors must tell the vendors/providers of the contractor's local Host Site ID and provide the additional CWF Host Site IDs for possible use in the event eligibility information is to be requested for a beneficiary whose records reside at a different host. Explain that an alternate Host Site ID will need to be submitted if they receive a message "Not Found" or "Not In File," to search any other Host Site. The CWF Host Site IDs are:

- GL – Great Lakes
- GW – Great West
- KS – Keystone
- MA– Mid- Atlantic
- NE – North East
- PA – Pacific
- SE – South East
- SO – South
- SW – South West

Since the Mutual Contractor is connected to all CWF Host Sites, Mutual's provider/vendors can use any of the Host IDs in the 270 files.

7. IVANS must:

    a. Contact each contractor to obtain a signed sponsorship agreement or addendum to an existing agreement, provide information on the nature and hours of help desk support IVANS will furnish providers/vendors, and clarify the process for future contractor-to-IVANS communication for connectivity related information, such as for contractor reporting of any subsequent IP address changes. The sponsorship agreement will permit IVANS to have dummy access to enable testing of their connection through the MDCN to the data center;

    b. Obtain a signed customer communication agreement (see attachment 2) that includes fees from the provider/network service vendor, and arrange for direct payment from the provider/vendor for their connectivity services;

    c. Furnish providers/network service vendors with the software, user ID and password for use of the IVANS telecommunication lines. IVANs estimates that it will take approximately two weeks to establish connectivity for dial-in users and providers/vendors with existing IVANS accounts, and 60 days for dedicated users that will need a circuit installed;

    d. Inform the provider/vendor of those error messages that will be issued in the event connection is attempted but is unsuccessful, how to identify that the message is from IVANS, rather than Medicare, and corrective action to be taken in the event of receipt of each of those messages; and

    e. Establish a means to require their client providers to update their password every 60 days at a minimum.

    f. Provide deployment, installation, and help desk first level support services to all providers and network service vendors that contract with IVANS.

    g. Notify the vendors/providers of the hardware and software requirements for connectivity.

8. A provider not using DDE for eligibility data access, or a network service vendor must:

    a. Submit a small number of 270 queries in production mode via IVANS, their private network, or LU6.2 connection via the MDCN through the data center and the CWF security module to the CICS region as a live test. Once transmission is successful, full transmission of 270 queries may commence;

b. If unable to connect as result of an IVANS, private network, or LU6.2 problem, take action to resolve as directed by IVANS, the private network, or the LU6.2 administrator;

c. If connected to the data center by IVANS, private network, or LU6.2, but the CWF security module is unable to identify the provider/vendor, a proprietary message is generated by the CWF module and routed back to notify the provider/vendor of the reason the request is being rejected. Action must be taken as directed by the contractor under step 6;

d. If unable to obtain eligibility verification as the CWF module determines 270 standard syntax requirements are not met and a 997 is issued, proceed as directed by the contractor under step 6;

e. If unable to obtain eligibility verification as the CWF module determines 270 implementation guide semantic requirements are not met, and a proprietary error message is issued, proceed as directed by the contractor under step 6;

   i. If the provider/vendor searches for an error in their software that contributed to syntax or semantic errors, but contends that the CWF module is in error (a possibility during initial testing), this must be reported to the contractor for further investigation.

f. If an abend message received from the CWF module, resubmit the query the next day. If another abend message is received, contact the contractor for further information or investigation.

9. The contractor must:

   a. Have an access facility to view Virtual Storage Access Method (VSAM) files (see the April and July 2003 CWF release specifications);

   b. Access a copy of the submitted query and the response from the VSAM report (April 2003) or from VSAM directly (see the July 2003 CWF release specifications) if the provider/vendor alleges the CWF module is at fault;

   c. Diagnose to determine whether CWF or the provider/vendor software is actually at fault (report the error to the CWF host or the CWF beta site per existing practice to open a Problem Log (PLOG) if a CWF module error is suspected);

   d. Determine if previously notified of CWF actions that might have resulted in an abend situation and when the problem is expected to be corrected;

   e. Report the CWF abend information to their CWF Host contact if no prior notification received of the condition; and

f. Notify the provider/vendor of the findings of the investigations and/or of corrective action being taken.

10. The CWF maintainer must:

a. By April 7, 2003, modify the software to write all 270s that encountered an error resulting in a proprietary message, 997, TA1 or 271 with AAA03, and successfully issued 271s to a separate VSAM file with key elements preceding the record for sorting and selection purposes. Contractors must be able to request a report from the VSAM file to indicate error or transaction detail, and must be given the capability to set parameters to select specific data for reports to be generated from JCL streams. The software must also create backup/reorganization jobs for the new VSAM files. The data must be retained for 30 calendar days to enable contractor review as needed, and automatically be purged at the end of 30 calendar days. Contractors must be able to request that a report to be run at their data center and either shipped to the contractor or viewed online via Time Sharing Option (TSO).

b. By July 1, 2003, modify the software to also be able to create an online display feature for the data captured on the VSAM files that will comprise several CICS Maps for displaying 270, 271, 997, TA1, and proprietary error segments in detail. Specifications for these files must be supplied to Skosko@cms.hhs.gov by June 1, 2003, to be shared with the Medicare contractors and posted to the HIPAA EDI Web site. A menu screen must be furnished to enable a contractor to selectively view data as soon as a problem may be reported in the same CICS region. Contractors must also be able to screen print data online. Furnish the data centers with error messages to be generated in specific error conditions detected by the CWF modules that prevent processing of the request for eligibility verification;

c. Work with the data centers and the contractors to expeditiously correct any errors detected in operation of those modules during testing; and

d. Separately record the number of unique 271 responses that did not contain an AAA segment generated per calendar month per contractor, and DDE eligibility responses furnished per calendar month per contractor and supply those numbers to the data center through which the 271 or DDE data was channeled within five calendar days of the end of each month. Eligibility queries submitted with a "T" indicator for a test are to be treated the same as "P" indicators when calculating the 271 count.

e. CMS will post the 270 CWF eligibility module and the module 271 maps used by CWF for translation purposes at: www.cms.hhs.gov/providers/edi.default.asp for the benefit of network service vendors or providers that may have a need for that information.

f. Establish a timed-out feature to disconnect a submitters connection if no new files are sent within five seconds after the previous 271 file was returned.

11. Shared System maintainers must:

a. Either furnish bridge software to enable providers/vendors to view the CWF eligibility screen through their DDE connection, or to direct providers/vendors to connect to the ELGA or ELGB screens to obtain eligibility information. The Fiscal Intermediaries are exempt from this requirement at this time. This requirement is specific to the carriers, only.

b. Provide software to the data centers that will:

i. Calculate the number of 271s and DDE eligibility responses combined together generated per quarter per contractor per provider and forward the total of 271s to each contractor;

ii. Calculate a ratio per provider per contractor of the number of 271s and DDE eligibility responses issued in a quarter per the number of claims processed for that provider for that contractor that month Exclude the number of failed (status information value code of F) from the CWF audit trail module from the ratio calculation; and

iii. Have that software issue a report to the contractors within 10 business days of the end of each quarter with the numbers used in the ratio calculations per provider and the ratio for each provider

12. A data center, including MDC1 and MDC2, must:

a. Take corrective action as needed to fix any errors detected during testing of the security and eligibility modules that were shipped with the R2003100 January CWF release for the carriers and the R2002300 July release for the intermediaries. The software provides a back end interface to validate the CICS User ID and password prior to reading 270s. The password "prompting" is done at the data center of the contractor.

b. Maintain a Transmission Control Protocol/Internet Protocol (TCP/IP) connection with MDCN and a CICS TCP/IP socket interface for the CICS region(s) where the CWF eligibility data will reside. This is required to receive and send these eligibility transactions and related error messages (CMS will supply the MDCN with the TCP/IP address for each data center);

c. Run the CWF shared software "One-Timers," a special JCL job provided by the CWF maintainer to create security and audit files for the contractors' CICS regions;

d. Load and test the eligibility software supplied by their shared system maintainer;

e. Issue and update ID numbers and passwords, and coordinate password problem correction, such as reactivation of a frozen password, with their contractors; and

f. Load software as supplied by the CWF maintainer that will afford contractors the ability to view VSAM files containing eligibility queries and responses to facilitate error diagnosis and correction.

g. Monitor the socket usage to determine if additional sockets are needed to accommodate current and future traffic.

13. The contractor must:

a. Review the provider inquiry to claim ratios monthly and take action as needed to correct or prevent potential abuse situations detected by the ratios. If the inquiry to claim ration is higher than 100, i.e., if there were 100 or more inquiries for every 70 claims submitted by that provider, the contractor must investigate to determine if there is a legitimate explanation for the imbalance and explain Medicare's inquiry volume expectations and restrictions if there appears to be a problem with excess eligibility queries. If there is a problem, or the behavior continues, the contractor must suspend that provider's online access to eligibility data for 1-year from the date of determination of abuse. At the time of suspension, the provider must be notified that it may apply for restoration of access privileges at the end of that year. Do not restore electronic access unless requested by the provider;

b. Include the 271 total supplied by the data center for the quarterly report.

10.3 - Eligibility Query Types

(Rev. 1, 10-01-03)

A. Direct Data Entry (DDE) Eligibility Screens

Contractors that currently support a DDE screen for provider access to eligibility data are to continue to support this functionality. DDE eligibility screen functionality is not to be established where the capability does not already exist. Shared system maintainers are to furnish the data centers bridge software in their April 2003 release to enable providers to directly view the CWF eligibility screen in real-time, in lieu of any prior proprietary DDE eligibility screen, unless instructed otherwise by CMS. When a provider selects the DDE eligibility menu option, the provider must view the CWF eligibility screen. Providers that elect to use a DDE screen for eligibility data, where supported, are responsible for connection costs related to use of the screen.

The CWF ELGA screen will replace HIQA and HUQA, and the ELGH screen will replace HIQH. CWF has modified the managed care HIHO screens to match the data content for the ANSI X12N 271 transaction.

B. LU6.2

Carriers do not provide LU6.2 connections. Intermediaries contractors with current LU6.2 capability can continue to support LU6.2 if cost effective and those users elect to continue to obtain eligibility data via that connection. Do not establish LU6.2 connectivity if not previously supported and do not add LY 6.2 users. Intermediaries must support TCP/IP connection through IVANS, however, in addition to LU6.2. The LU6.2 connection must be via the MDCN and the contractor's data center through the CWF security module to the appropriate CWF CICS region and port, if applicable. All eligibility queries submitted via the LU6.2 connections must be in real-time and submitted in ANSI X12N 270 version 4010A.1 by October 16, 2003. Real-time responses will be returned to the submitters in the ANSI X12N 271 version 4010.A1 format, or an error message format, via the same LU6.2 connection. Providers that choose connection via LU6.2 are responsible for their internal programming to support this connection and any costs related to use of that connection.

C. Private Network Connections

In some cases, contractors had previously established connections via private networks to enable providers and network service vendors to obtain eligibility data. If a contractor elects to continue to support private network connections, the connections must be modified as necessary by October 16, 2003, to connect via MDCN through the contractor's data center and the CWF security module to the appropriate CICS region and port, as applicable. All eligibility queries submitted via a private network must be in real-time and submitted in ANSI X12N 270 version 4010A.1 by October 16, 2003. Real-time responses will be returned to the submitters in the ANSI X12N 271 version 4010A.1 format, or an error message format, via the same private network connection. Users of private networks are responsible for payment of the network service provider for the costs of their connection and of any services obtained from that network.

D. IVANS

IVANS is an agent for establishment of AT&T private network connections. IVANS can supply direct connections for eligibility data retrieval to those providers and network service vendors that have been authorized to access this data electronically, and that have chosen not to exclusively use DDE, LU6.2, an ARU, or alternate non-electronic means that may be supported to verify beneficiary eligibility. Each contractor must offer providers and network service vendors the option to connect via IVANS in lieu of connection via private network or other means. Some providers may already have IVANS connectivity established.

IVANS is not the only private network reseller qualified to establish connectivity of this type. Requests involving the use of connections via other telecommunication companies can be considered if they meet certain criteria. Refer requests by providers or network service vendors for connectivity via an alternate private network to Skosko@cms.hhs.gov for review and determination.

The decision of which means of connection best meets a provider's needs is to be made by individual providers. As with the private networks and LU6.2, when supported, IVANS connections will be to the CWF CICS region via the MDCN, the data center, and the CWF security module. All eligibility queries submitted via IVANS must comply with ANSI X12N 270 version 4010A.1 and be real-time. Medicare will return real-time responses in the ANSI X12N 271 version 4010A.1 format or the appropriate error transaction. Providers and network service vendors electing to use IVANS are responsible for payment of the costs related to use of the connection. Every Medicare contractor must offer IVANS as an option for provider and network service vendor connection.

E. Network Service Vendors

Providers will continue to have the option to contract with network service vendors that have been approved by Medicare to act as agents to route beneficiary eligibility data between Medicare and the providers. Network service vendor requirements are specified in Chapter 24. This PM is not modifying the network service vendor requirements. These vendors must also be given the option to connect via IVANS, rather than a previously existing connection, to obtain beneficiary eligibility data on behalf of their provider clients.

Providers that elect to contract with network service vendors are responsible for the cost of services they obtain from those vendors. Eligibility queries submitted by network service vendors must be real-time in the ANSI X12N 270 version 4010A.1 format by October 16, 2003. Contractors will send real-time ANSI X12N 271 version 4010A.1 responses in return, or appropriate error report transactions if applicable. Batch queries and responses will not be supported Medicare. Vendors may, however, reformulate inquiries received in batch from a provider client into a string a real-time queries, and likewise reformulate real-time responses from Medicare into batches if requested by their clients.

Network service vendors must be issued a separate user ID and password for each CICS region to be accessed on behalf of their clients.

F. ANSI X12N 270/271 version 4010A.1

The implementation guide for the transactions can be downloaded at www.wpc-edi.com/HIPAA. For any questions regarding the CWF data elements, please refer to the CWF Web site: http://cms.csc.com/cwf/. In addition, the list of data elements with definitions is posted to the following Web site: www.cms.hhs.gov/providers/edi/default.asp .

1. The eligibility security module will use the following data elements to validate authority to access the CWF eligibility data:

    a. Contractor number;

    b. Provider number

    c. Submitter number;

    d. Submitter name;

    e. Submitter contact name;

    f. Date created;

    g. Time created;

    h. Date last updated;

    i. User ID last update;

    j. EDI enrollment form (Y or N);

    k. Network service agreement (Y or N);

2. The following data elements will be used by CWF to process an eligibility query:

    a. Health Insurance Claim Number (HICN);

    b. Surname;

    c. First Name;

    d. Date of Birth;

    e. Sex;

    f. Contractor Number;

    g. Provider Number

    h. Requester ID (submitter ID);

    i. Usage Indicator (P/T);

    j. Applicable Date; and

    k. Host ID.

The first three data elements must be entered correctly in the 270 at a minimum to enable a 271 to be generated for error reporting. Otherwise, a 997 or TA1 will be issued.

3. All professional providers, including retail pharmacies, authorized to receive eligibility data will be issued the same data set. Medicare will not accept eligibility queries submitted in a National Council of Prescription Drugs Plan format at this time. The following data elements will be included in the professional 271 response as applicable:

   Contractor Number

   Provider Number

   Requester ID

   Date & Time Stamp

   Surname

   First Initial

   HICN

   ZIP Code

   Date of Birth

   Date of Death

   Sex Code

   Applicable Date

   Current Part A Entitlement Date

   Current Part A Termination Date

   Current Part B Entitlement Date

   Current Part B Termination Date

   Managed Care Plan ID Code

   Managed Care Plan Option Code

   Managed Care Plan Entitlement Date

   Managed Care Plan Termination Date

Other Program Entitlement

a. Workers Compensation

b. Black Lung

MSP Data (can occur up to 5 times)

a. MSP code

b. MSP effective date

c. MSP termination date

d. MSP insurer's name

e. MSP insurers address

f. MSP insurers city, state, zip

Lifetime Reserve Days

Part A Spell Data

a. Hospital days remaining

b. Coinsurance hospital days remaining

c. SNF days remaining

d. Co-insurance days remaining

e. Inpatient deductible remaining

f. Date of earliest billing action

g. Date of latest billing action

Part B Spell Data

a. Most recent Part B year

b. Part B cash deductible remaining

c. Part B physical/speech therapy limit remaining

d. Part B occupational therapy limit remaining

Hospice Period Number

Hospice Start Date

Hospice Termination Date

Pap Risk Indicator

Pap Date

Mammography Risk Indicator

a. Mammography date
b. Screening risk indicator
c. Technical or professional
d. Recent dates

Glaucoma Risk Indicator

a. Technical or professional
b. Recent dates

Colorectal Risk Indicator

a. Technical or professional
b. Recent Dates

Prostrate Risk Indicator

a. Technical or professional
b. Recent dates

Pelvic Risk Indicator

a. Technical or professional
b. Recent dates

ESRD First Code

ESRD Effective Date

Transplant Indicator

Transplant Discharge Date

HHEH Data (current two episodes)

a. HHEH start date

b. HHEH end date

c. HHEH date of earliest billing action

d. HHEH date of latest billing action

HHBP Date (current two episodes)

a. HHBP start date

b. HHBP end date

4. All fee-for-service institutional providers, excluding Home Health (HH) and Managed Care Organizations (MCO) receive the same 271 basic data set, as applicable:

Contractor Number

Provider Number

Requester ID

Date & Time Stamp

Surname

First Initial

HICN

ZIP Code

Date of Birth

Date of Death

Sex Code

Applicable date

Current Part A Entitlement Date

Current Part A Termination Date

Current Part B Entitlement Date

Current Part B Termination Date

Managed Care Plan ID Code

Manages Care Plan Option Code

Managed Care Plan Entitlement Date

Managed Care Plan Termination Date

Other Program Entitlement:

a. Workers Compensation
b. Black Lung

MSP Data (can occur up to 5 times

a. MSP code
b. MSP effective date
c. MSP termination date
d. MSP insurer's name
e. MSP insurer's address
f. MSP insurer's city, state, zip code

Lifetime Reserve Days

Part A Spell Data:

a. Hospital days remaining
b. Coinsurance hospital days remaining
c. SNF Days Remaining
d. Coinsurance SNF days remaining
e. Inpatient deductible remaining
f. Date of earliest billing action
g. Date of latest billing action

Part B Spell Data:

a. Most recent Part B year
b. Part B cash deductible remaining
c. Part B physical/speech therapy limit remaining
d. Part B occupational therapy limit remaining

Hospice Data:

a. Period Number
b. Hospice Start Date
c. Hospice Termination Date

Pap Data: Pap Smear Data

a. Pap Risk Indicator
b. Pap Date

Mammography Data:

a. Mammography Risk Indicator
b. Mammography Date

Screening Data:

a. Screening risk indicator
b. Technical or professional
c. Recent dates

ESRD Data:

a. ESRD First Code
b. ESRD Effective Date
c. Transplant Indicator
d. Transplant Discharge Date

HHEH Data (current two episodes):

a. HHEH start Date

b. HHEH end date

c. HHEH date of earliest billing action

d. HHEH date of latest billing action

HHBP Date (current two episodes)

a. HHBP start date

b. HHBP end date

5. All institutional psychiatric providers will receive the basic data set plus the following additional data elements: Lifetime psychiatric days remaining and Part B psych limit remaining. CWF will identify institutional psychiatric providers by the "4" in the third digit of the provider number.

6. All home health providers will receive the following data set:

Contractor Number

Provider Number

Requester ID

Date & Time Stamp

Surname

First Initial

HICN

ZIP Code

Date of Birth

Sex Code

Applicable Date

Date of Death

Current Part A Entitlement/Termination Date

Current Part B Entitlement/Termination Date

Managed Care Plan Data:

a. Managed Care Plan ID code
b. Managed Care Plan option code
c. Managed Care Plan entitlement code
d. Managed Care Plan termination date

Other Program Entitlement: Workers Compensation or Black Lung

MSP Data:

a. MSP code
b. MSP effective date
c. MSP termination date

Hospice Data (last four occurrences):

a. Hospice period number
b. Hospice start date
c. Hospice termination date
d. Provider Number
e. Intermediary Number

HHEH Data (current two episodes):

a. HHEH start date
b. HHEH end date
c. HHEH date of earliest billing action
d. HHEH date of latest billing action
e. Patient Status
f. Cancel Indicator
g. Intermediary Number

h. HHEH provider number

HHBP Data (current two periods):

a. HHBP A visits remaining

b. HHBP B visits applied

c. HHBP earliest billing date

d. HHBP latest billing date

7. Managed Care plans will receive two separate types of eligibility responses, depending on whether the beneficiary is a member of the plan:

   a. HMO Eligibility Response Data Set:

      Contractor Number

      Provider Number (Managed Care Plan ID)

      Requester ID

      Date & Time Stamp

      Surname

      First Initial

      HICN

      Date of Birth

      Date of Death

      Sex Code

      Applicable Date

      County/State Code

      Current Part A Entitlement/Termination Date

      Current Part B Entitlement/Termination Date

      MSP Data (can occur up to 5 times):

         MSP code

         MSP effective/termination date

Insurer’s name, address, city, state, zip code

Validity/delete indicator

Original contractor

Updating contractor

Date of accretion

Patient relationship code

Policy number

Group number

Group name

Maintenance date

Insurer type

Hospice Data (last 4 occurrences):

Hospice period number

Hospice start date

Hospice termination date

ESRD (yes or no)

b. HMO Eligibility/Utilization Response Data Set - In addition to the data in the HMO eligibility response above, the following data elements will be furnished as applicable:

Lifetime Reserve Days

Lifetime Psychiatric Days remaining

Home Health Agency Visits (A remaining, B applied)

Spell of Illness (Part A):

Hospital days remaining

Coinsurance hospital days remaining

SNF days remaining

Coinsurance SNF days remaining

Inpatient deductible remaining

Date of earliest billing action

Date of latest billing action

10.4 - Intermediary and Carrier Responsibilities

(Rev. 1, 10-01-03)

A. Contractors notified CMS prior to February 2003 of the name of a staff member designationed as responsible for IVANS coordination, contact information for the staff member, and the IP address and name of their data center. CMS shared this information with IVANS. Contractors must notify IVANS immediately of changes in the identity of or contact information for that person(s), as well as of changes to data center IP addresses and ports as that would impact the IVANS connections.

VANS was to inform each contractor in February 2003 of the process to update that information, and to obtain a sponsorship agreement from each contractor. In the sponsorship agreement, a contractor certifies that they will have pre-approved each provider and network service vendor that they refer to IVANS to receive beneficiary eligibility data via the IVANS connection, and that IVANS will be notified if the contractor becomes aware of a reason to rescind or modify that approval. Contact rex.bevis@ivans.com or phone 513-271-5668, if contractor has not yet received that information from IVANS or has not yet submitted a signed sponsorship agreement. (See workflow items 6 a, b, c.)

B. Contact the contractor data center to determine those hours and days when the data center will process real-time eligibility queries. At a minimum, this support is to be furnished during the same hours that the contractor has EDI support hours. Establish a procedure with the data center to notify you of changes to IP addresses, and to coordinate reporting of any CWF module problems detected during limited beta testing of selected providers and/or network service vendors on 270/271 transmission. Establish a timeline with your data center as to when connections will be established, CWF modules loaded, related shared system maintainer releases loaded, and VSAM files available to enable limited provider testing to begin. (See workflow item 1.d.)

Include information in the next regularly scheduled provider bulletin and on the contractor's Web site to notify providers of/that (see workflow items 1a, 2, 6d, f; it is not necessary to reissue any portions of this information that may have been shared with providers prior to receipt of this PM):

1. The options for provider and network service vendor connectivity to obtain eligibility data, i.e., IVANS, DDE, and LU6.2, private network,

ARU if supported, or via other non-electronic means if supported to obtain such information.

2. If DDE is supported for eligibility, changes they can expect to see in the eligibility screen and when.

3. Action to be taken by providers/network service vendors interested in establishment of an IVANS connection.

4. If a private network is supported, any changes in their connection process that would require action by the provider.

5. ANSI X12N version 4010A.1 270 queries only will be accepted for eligibility data via IVANS, private networks if you support, and LU6.2 if you support by October 16, 2003.

6. ANSI X12N 271 version 4010A.1 responses, or error reporting transactions including the 997, TA1, and contractor proprietary format will be issued as applicable.

7. No other query or response formats for electronic eligibility data, other than via DDE, will be supported by Medicare effective October 16, 2003.

8. Eligibility queries are to be submitted and responses issued in real-time only; batch transactions will not be accepted by Medicare.

9. Unless Medicare is notified otherwise, providers and vendors will be kept on the same connection for eligibility data as at present, but that transmission of non-271 eligibility data will cease.

10. Providers/vendors must notify Medicare immediately if there is a change in their election of a network service vendor.

11. Providers and vendors are responsible for the cost to establish and maintain connections to obtain beneficiary eligibility data. IVANS or another private network administrator will bill providers directly for these costs. Payments are not to be submitted through Medicare.

12. Providers can elect to contract with a network service vendor to obtain electronic beneficiary eligibility data on their behalf. Providers are responsible for payment of the vendor’s charges for those services.

13. Providers must file a compliant EDI agreement with the contractor, prior to Medicare’s transmission of eligibility data to a vendor on their behalf.

14. Providers that have contracted with a network service vendor must furnish the contractor a signed statement that they have authorized that vendor to obtain eligibility data on their behalf. A copy of the agreement the

provider signed with the network service vendor can be used in lieu of the signed statement.

NOTE: The contractor must populate the CWF security module at the data center with information for each provider that will continue to access eligibility data using an existing LU6.2, private network, or DDE connection.

15. Home health episode periods, home health benefit period and managed care plan information will now be available in 271 responses and the new DDE eligibility screen, where supported, but will not be available via ARU.

16. Although Medicare furnishes providers with basic information on the HIPAA standard transaction requirements to enable providers to make educated and timely decisions to plan for use of a HIPAA standard, Medicare will not furnish in-depth training on the use and interpretation of standards implementation guides. Providers that feel their staff have a need for such training are expected to obtain that training from commercial vendors or standards development organizations.

17. How to contact the contractor to obtain further information or to arrange for IVANS connectivity.

18. Any other information the contractor considers of value to a provider contemplating use of the 270/271.

Share this information with network service vendors, billing services, and provider clearinghouses also. Notify the network service vendors that Medicare privacy rules prohibit inclusion of user IDs and passwords within a 270 or 271 transaction. Authentication must occur outside of the transaction. For eligibility data purposes, clearinghouses authorized to collect eligibility data on behalf of providers are also considered network service vendors and must sign a network service vendor agreement. Billing agents that do not provide translation services are considered provider subcontractors. Although billing agents must sign an agreement with the providers to safeguard beneficiary specific data that may be accessed, a billing agent is not considered a network service vendor for eligibility access purposes and is not required to sign a network service agreement.

D. Obsolete

E. If a provider or network service vendor expresses interest in establishing an IVANS connection for eligibility data:

1. Obtain an EDI agreement from the provider, if not already in file. (See workflow items 3 and 5. If the provider will not also submit claims electronically, modify the EDI agreement to exclude claim specific requirements.)

2. If a network service vendor is involved, obtain either a signed statement from the provider authorizing that vendor to collect the eligibility data on behalf of the provider or a copy of their network service agreement. The provider must agree to notify you if that agreement is rescinded or modified. (See workflow item 3.)

3. Have the network service vendor sign a network service agreement if not already in file, agreeing to safeguard the data transmitted. (See workflow items 3 and 4.)

4. Evaluate the request to certify that there is no history of abuse or other cause that would lead you to disapprove electronic access by this provider/network service vendor to beneficiary eligibility data. (See workflow item 6b.)

5. If no objection to a connection (see workflow items 6c, d, e):

   a. Notify IVANS as directed in your sponsorship agreement of the name of and contact information for the provider or network service vendor approved to receive eligibility data from Medicare electronically. The IVANS Agreement will be executed directly between the provider/vendor and IVANS. The contractor will not be a party to this agreement between the provider and IVANS. Forward IVANS the IP address, and any port number incorporated in the client address, for the provider's CICS region. If there is a network service vendor, a separate IP address and any port numbers must be furnished for each CICS region the vendor is authorized to access on behalf of client providers.

   b. Populate the CWF security file residing at the data center with information on the provider and any related network service vendor.

F. Provider and Network Service Vendor Connections

Real-time 270s are to be submitted as one ISA-one GS-one ST-one SE-one GE, and one IEA. Repeat the prefix data prior to transmission of each 270. Submission of multiple GS and ST segments is permitted only when the batch structure is used, and Medicare does not support the batch structure. A real-time response is received for each 270, either a 271 or an error report, prior to transmission of the next 270.

G. The CWF beta site and contractors with DDE capability must test the CWF modules when loaded. Contractors without DDE capability will not be able to test that software. All contractors are to perform routine release testing of shared system releases containing eligibility-related modifications. Follow existing procedures to report potential errors detected in the software.

H. Provider Testing

1. Contractors must beta test with a small number of providers and/or network service vendors before putting large numbers of providers/vendors into production for 270/271 transactions, regardless of the mode of transmission. Beta testing of this nature must be conducted for DDE, LU6.2, and private networks

supported by a contractor, as well as IVANS, once the CWF security and eligibility modules are installed, populated, and operational. This beta testing must begin by July 11, 2003.

2. Once that beta testing is successful, those providers may submit all of their eligibility queries via that connection in production mode, and other providers/vendors can be notified to begin submitting eligibility queries in production mode.

3. Contractors are not expected to individually test with each prospective 270/271 user, but are to likewise direct each user to initially submit a small quantity of 270 queries and for those submitters to certify their transmissions have been successful prior to sending all of their eligibility queries in production mode.

I. Contractors must accept requests from both participating and non-participating providers and their network service vendors for electronic access to eligibility data.

10.5 - Data Center Responsibilities

(Rev. 1, 10-01-03)

A. Data centers must inform their contractors of the days and hours when they will be able to support eligibility queries. The days and hours are to be the same for each contractor supported by a specific data center. Support must be supplied at a minimum for the same hours that a contractor is required to provide electronic media claims support to submitters.

B. Data centers can refer to the following procedures for TCP/IP installation:

1. IBM Book TCP/IP V3R2 for MVS: CICS TCP/IP Socket Interface Guide, Document Number: SC31-7131-03. Chapters one and two have instructions on setting up and configuring CICS TCP/IP. This book also covers the installation of enhanced native TCP/IP sockets for CICS available on OS/390 V2.4 and above. They are valid for CICS R4.1 and CICS TS 1.2 and above.

2. Online Library Omnibus Edition, OS/390 Collection (SK2T-6700) and the IBM Intranet athttp://publibz.boulder.ibm.com.

C. The data center must establish IP addresses and port numbers for providers that contractors have approved to receive eligibility data electronically. The data center must establish one port for the socket interface.

D. The data center must establish a CICS user ID and password for each provider to allow that provider, or the provider's network service vendor, to access to the CICS region for real-time 270/271 processing, and coordinate password problem correction, such as reactivation of a frozen password, with their contractors.

E. The data centers will use a security package for user authentication. The CWF software security application will only validate against the security packages defined as follows:

1. RACF;

2. ACF2; or

3. TOP SECRET.

F. The data center must install CWF software at the CICS regions where CWF Carrier eligibility transactions may be processed, and:

1.Define PCT entry for IBM Listener transaction "ELGV" module ELGXSTTC for Part B;

2.Define PCT entry for IBM Listener transaction "ELGU" module ELGXSTTC for Part A;

3.Define PCT entry for transaction "ELGL" module ELGXSTLU for Part A via LU6.2.

G. The data center must delete any of the providers on the CWF security module, which the provider enrollment department has deactivated or terminated due to no claims submissions, sanctions, leaving a practice, etc. If the provider can no longer be paid by Medicare, then the provider must be taken off of the CWF security module so that the provider/vendor can no longer obtain eligibility information.

H. To minimize bandwidth and connectivity time for real-time eligibility queries submitted by vendors, do not disconnect a submitter between transactions unless 5 seconds has elapsed since transmission of a 271, 997 or TA1. Allow multiple 270s to be transmitted in series during a single connection session, with a 271 or error response received after each 270. CWF will be simultaneous processing 270s from multiple submitters and will process each 270 and 271 (or error message) as a discrete action. CWF will not be able to differentiate to determine whether each discrete 270/271 processed is for the same submitter. As a result, CWF will require transmission of the prefix data to revalidate for each query.

10.6 - Provider/Network Service Vendor's Responsibility

(Rev. 1, 10-01-03)

A. Providers must notify the contractor of any change in their network service provider or telecommunications provider. Vendors must notify the contractor of any changes in their telecommunications provider.

B. It is the provider's/vendor's responsibility to develop or obtain a client TCP/IP (streaming socket) program to connect with Medicare to obtain this information electronically by means other than DDE.

   1. This must be a non-SSL connection. Encryption is not required is this situation as only dedicated private lines may be used for telecommunication.

   2. The TCP/IP socket program will use the Client-Listener-Child-Server model.

   3. Providers are to obtain commercial services if they require assistance to install the client TCP/IP streaming socket. This service will not be furnished by Medicare.

C. It is also the provider's/vendor's responsibility to obtain ANSI X12N compliant 270/271 version 4010A.1 software for submission and receipt of eligibility query data, and for receipt of a 997 and TA1. This software will not be supplied by Medicare.

   1. It is not Medicare's responsibility to beta test or diagnose extensive numbers of flaws in their eligibility software. Contractors will supply reasonable support to enable a provider or vendor to establish connectivity for eligibility queries, but it is not reasonable to expect a contractor to repeatedly diagnose problems incurred by a provider/vendor when the contractor has determined that the problems being experienced are the result of numerous flaws in the software being used by the provider/vendor.

   2. In those cases, providers/vendors must have their software problems corrected and their software internally tested prior to resubmission of eligibility queries to Medicare.

D. Transmission instructions:

   1. The provider/vendor must transmit "ELGV" to request the carrier data center or "ELGU" to request an intermediary data center to initiate the host server program. Samples of client TCP/IP programming are located at:

      http://publibz.boulder.ibm.com/cgibin/bookmgr/library Manual CICSTCP/IP Sockets Interface Guide, Document Number SC31-8518 and

      http://msdn.microsoft.com for sample Microsoft Winsock Applications.

   2. Providers/vendors with current LU6.2 connectivity will need to modify their software to use the following connection identifiers. The "sendsize" and "receivesize" has been defaulted to the largest 270/271 data record. These fields may be modified as appropriate.

      Netname : ILU.NETNAME ←=== **Modename** : DIADWCSI

Session Properties:

Protocol	: Appc	Appc	Lu61	Exci
Maximum	: 010 , 001	0-999		
SENDSize	: 12000	1-30720		
+ RECEIVESize	: 12000	1-30720		
Transaction	: ELGU			

3. Since the data center is required to validate a vendor’s and provider’s identity prior to processing the 270 request, the user ID and password issued by the data center for a specific CICS region, must be prefixed as follows prior to the start of a transmission of 270 data for that CICS region for a specific provider. Data can be in upper or lower case.

Data Element	**Description**	**Bytes (66)**	**Content**
Transaction	Transaction ID	04 Characters	“ELGV” for PartB “ELGU” for Part A “ELGL” for Part A LU.6.2 for TCP/IP Start 270 Processing
Transaction	Unique Record Identifier	30 Characters	Record Identifier
User ID	User ID provided by the data center for that CICS region	08 Characters	Provider or Vendor ID
Password	Password provided by the data center for that CICS region	08 Characters	Current Password

Password1	New password when changed by user	08 Characters	New Password
Password2	New password verification	08 Characters	New Password
270 data follows	ISA and other segments		

The security prefix data element information follows:

a. The transaction ID “ELGV” identifies a record as a professional eligibility transaction issued via TCP/IP. The transactions ID “ELGU” identifies a record as an institutional eligibility transaction issued via TCP/IP. The transaction ID “ELGL” identifies the record as an institutional transaction issued via LU6.2.

b. Providers/vendors that process asynchronous eligibility transactions may utilize the Transaction Reference No. data element to uniquely identify each 270. The Transaction Reference No. will allow the organization to match the CWF response with the corresponding 270 query if CWF is unable to read/translate the submitted 270.

c. Providers/vendors are required to send their user ID and password prior to submission of each 270.

d. Providers/vendors will periodically be prompted to change their passwords, and must self-initiate a change in password if there has been a change in personnel granted access to the eligibility records or a potential breach in security. To change a password, set the Password field to the old password, and insert the new password in the Password 1 and Password 2 fields.

4. Upon successful authentication, the 270s will be routed to the CWF eligibility module for response.

5. CWF will return a 271, 997, or a TA1, prefixed with the following proprietary record format in response to a processed 270. Either 271, 997, or TA1 will follow the prefix. The layout for the 271, 997 and TA1 formats is located in the version 4010A.1 270/271 implementation guide that can be downloaded at www.wpc-edi.com/HIPAA. This proprietary format will also be used in situations when login has failed the data center user authentication process; or when CWF is unable to read/translate the 270 data. Error messages related to data center security authentication and system abends will be returned in the CWF proprietary prefix layout in the Message Text of the response with the appropriate settings of Response-code and Message-code. The format of the CWF Response follows:

Data Element	**Description**	**Bytes(128)**	**Content**
Transaction TCP/IP	Transaction ID	04 Characters	“ELGV” – Part B
TCP/IP			“ELGU” – Part A
LU6.2			“ELGL” – Part A
Transaction Reference No.	Unique record identifier	30 Characters	Record Identifier
Date Stamp	System date	08 Characters	CCYYMMDD
Time Stamp	System time	06 Characters	HHMMSS
Response Code	Response code	02Characters	Return Codes
Abends	from CWF		“A” – System
			“E” – CWF Errors
			“F” – Password Verification Failure
Timeout			“T” – CWF
			“S” – Successful
Message Code	Error Code from CWF	08 Characters	EIBRESP and EIBRESP2
Message Text	Error Description	70 Characters	Error Description

Refer to the CWF Satellite Manual User documentation (OVERELGA, OVERELBG) for descriptions of the errors found on the following Web site: http://cms.csc.com/cwf/

6. Below is the description of the response prefix data elements.

   a. The transaction ID "ELGV" identifies the record as a carrier eligibility response via TCP/IP. The transaction ID "ELGU" identifies the record as an intermediary eligibility response via TCP/IP. The transaction ID "ELGL" identifies the record as an intermediary eligibility response via LU6.2.

   b. The Transaction Reference No. element from the 270 query prefix will be returned. This element can be used by the submitter organization to match the CWF response to the corresponding 270 query in the situation where CWF was unable to read/translate the incoming 270.

   c. The Date and Time stamp when the response was created will be populated in the prefix.

   d. The Response code will identify reasons for failure of the 270 query. This data element will notify the submitters of the 270 transaction the appropriate reasons for failure when CWF is unable to return either a 271/997 or a TA1 record. When the Response code is an "S" (Successful), the prefix will be followed with the subsequent 271/997/TA1 data.

   e. The Message code and Message Text elements will return the system failure codes and description of the Errors encountered.

7. If a system abend occurs, after successful translation of the 270 by CWF, the request will be returned as a 271 response under the 2000A level AAA Segment. The value to element AAA03 will be set to "42." The appropriate response code, error code and message will be returned in the 271 prefix layout.

8. CWF Application level security will be performed by validating the submitter and provider combination. Providers will be returned a TA1 record with error 006 - Invalid Interchange Sender ID.

10.7 - Supplemental CWF Module Information

(Rev. 1, 10-01-03)

A. The security module will contain the following information for the Intermediary:

   1. Provider Number;

   2. Submitter ID:

   3. Vendor Name:

   4. Vendor Contact Name:

   5. Date Created:

6. Time Created: Date Last Updated:
7. User ID Last Updated:
8. Provider Switch:
9. EDI Enrollment Form:
10. EDI Network Service Agreement (Y or N):

B. The security module will contain the following information for the carrier:

1. Carrier Number:
2. Provider Number:
3. Submitter ID:
4. Submitter Name:
5. Submitter Contact Name:
6. Date Created:
7. Time Created:
8. Date Last Updated:
9. User ID Last Updated:
10. Provider Switch:
11. EDI Enrollment Form (Y or N):
12. EDI Network Service Agreement (Y or N):

Audit information will be used by the data center to track the number of eligibility inquiries in relation to the number of claims submitted per provider. Unusual ratios that indicate more than 100 queries submitted per 70 claims must be investigated. Provider eligibility queries are intended to be used to enable successful submission of Medicare claims. The requesting of eligibility queries in excess of the number of claims could be a sign of misuse. Abuse can lead to a one-year suspension of electronic eligibility query privileges.

The audit trail module will contain the following information:

1. Audit Date;
2. Audit Time;

3. Submitter ID;

4. Provider ID;

5. HICN;

6. Record Type;

7. Transaction ID;

8. CWF Host Site;

9. Status Information Values are: “P’ – Pass or “F’- Fail

10. Contractor Number

10.8 - Eligibility Queries Options and Work Flows

(Rev. 1, 10-01-03)

NOTE: Although much of the workflow below refers to IVANS connectivity, direct data entry (DDE) connections are to continue where the capability currently exists. Private network and LU6.2 connections for eligibility data established by individual contractors can continue to be supported at the contractors discretion, but must also be routed to the appropriate CICS region through the MDCN and the data center. Private network and LU6.2 connection 270 queries are subject to the same CWF security verification and error reporting as indicated below for IVANS connections

15. The contractor must:

    a. Notify their providers and network service vendors of their eligibility options and of when the contractor is to be notified of changes that may impact their connection for receipt of eligibility data;

    b. Determine if any current LU 6.2 and private network connections used to furnish eligibility data electronically will continue to be supported.

    c. Submit a funding request to their Consortia Contractor Management Specialist (CCMS) HIPAA representative, with a copy to their regional financial management contact, within three weeks of the issue date of this PM for incremental costs related to implementation and FY 2003 operation of this eligibility inquiry process. This funding request must separately itemize incremental costs for:

        i. Assessed share of data center costs;

        ii. Submitter testing costs if not already submitted to CMS for HIPAA testing in general for FY 2003; and

iii. Other costs (itemize the “other” costs and identify the cost for each itemized activity).

d. Coordinate procedures for interaction with and for reporting of IP address and port changes with their data center.

16. The provider must decide whether to:

a. Continue to use DDE access to obtain eligibility data, where that functionality is furnished by their contractor. A CWF module operating at each data center will generate the screen eligibility data to be viewed via DDE. DDE will begin to report some additional eligibility data such as managed care coverage;

b. Continue to use LU 6.2 connection where it will continue to be supported to obtain 271 data;

c. Continue to use a private network connection, where it will continue to be supported, to connect to a data center to obtain 271 data;

d. Establish a direct connection with the data center via IVANS for use of the 270/271; or

e. Contract with a network service vendor that will channel eligibility data requests to/from the data center on behalf of the provider.

Whether the provider continues with a current connection methodology or changes to another connection methodology, the provider must notify the contractor of changes that would impact the information entered in the CWF security module.

17. If the provider decides to contract with a network service vendor, the provider must:

a. Sign an agreement with the network service vendor, that includes security and privacy specifications for the data, obtain passwords and ID numbers from that vendor for provider staff authorized to obtain the information, pay costs as assessed by the vendor, and load software from the vendor to establish that connection;

b. Furnish the Medicare contractor with a signed statement authorizing the network service vendor to act as their agent to obtain eligibility data, sign a Medicare Electronic Data Interchange (EDI) agreement with the contractor if not previously done, and agree to notify the contractor of any change in vendor or if they cease to use a vendor to obtain eligibility data.

18. The network service vendor must contact the contractor to sign a network service agreement.

19. If a provider decides to directly connect through IVANS, the provider must notify the contractor of their intent.

20. The contractor must:

    a. Sign a sponsorship agreement (which can be signed by an EDI supervisor or higher individual at the contractor, see Attachment 1) with IVANS agreeing to pre-clear all providers and network service vendors referred to IVANS for connectivity for eligibility data (contractors are to contact rex.bevis@ivans.com or phone 513-271-5668 within 2 weeks of the date of this PM if not yet contacted by IVANS concerning the sponsorship agreement);

    b. Determine whether the provider and/or network service vendor should be allowed to connect to the data center to obtain eligibility data. Contractor uses the same criteria that would previously have been used to determine whether a provider or network service vendor should have been given access to the eligibility data through the contractors front end;

    c. Notify IVANS of the contact information for an approved provider/network service vendor;

    d. Populate the provider's/network service vendor's information into the CWF security module (see the CWF specifications located on the following Web site: http://cms.csc.com/cwf/) that resides at the data center, and request a user ID and password from the data center for the pertinent CICS region(s). Where a port number is also needed for further identification, that number will need to be identified as part of the client address as MDCN cannot read port numbers in a network layer. The contractor must furnish the user ID and password to the provider, or the provider's designated network service vendor. The user ID is for the use of the 270 submitter, either the provider or the network service vendor as applicable;

        j. The contractor must also populate the CWF security module with information for those providers/vendors that will continue to use LU6.2, a private network, or DDE to access the CWF eligibility module, and update that file to reflect changes as needed.

        ii. The contractor must make any needed changes to their supported private network and LU6.2 connections that may be needed to enable interaction through the MDCN with the CWF modules residing at the data center.

        iii. The contractor must notify their private network and LU6.2 customers of any differences they will encounter in error messages received as result in this change in the source of the eligibility data.

e. Forward the IP address and port number as part of the client address where applicable for connection to the CICS region to IVANS (a vendor would be issued a separate IP address for each data center and a unique port number for each CICS region it is authorized to access);

f. Furnish the provider or vendor with information on:

   j. The proprietary messages that could be generated by CWF due to failure of the transaction to meet the implementation guide semantic requirements;

   ii. Situations when a TA1 would be issued and a description of the TA1 error codes, e.g., 006, that could be issued;

   iii. Situations when a 997 would be issued to report syntax errors in the transaction;

   iv. Situations when a 271 would be returned with error information, e.g., code 42 in AAA03 and an error code and message in the prefix;

   v. Action to be taken by the provider/vendor if any of those error messages is received.

   vi. Notify vendors/providers how to connect to the ELGA or ELGB screens to obtain eligibility information, if applicable.

   vii. Notify vendors/providers of the CWF Host Site ID, which must be inserted in ISA08 of the 270 transaction. The ISA07 must include the "ZZ' qualifier. Contractors must tell the vendors/providers of the contractor's local Host Site ID and provide the additional CWF Host Site IDs for possible use in the event eligibility information is to be requested for a beneficiary whose records reside at a different host. Explain that an alternate Host Site ID will need to be submitted if they receive a message "Not Found' or "Not In File", to search any other Host Site. The CWF Host Site IDs are:

      - GL – Great Lakes
      - GW – Great West
      - KS – Keystone
      - MA– Mid- Atlantic
      - NE – North East
      - PA – Pacific

- SE – South East
- SO – South
- SW – South West

Since the Mutual Contractor is connected to all CWF Host Sites, Mutual's provider/vendors can use any of the Host IDs in the 270 files.

20 - ANSI X12N 276/277 Claims Status Request/Response Transaction Standard

(Rev. 1, 10-01-03)

AB - 01-106

These instructions apply to intermediaries, carriers, durable medical equipment regional carriers (DMERCs), and their shared systems on Medicare requirements for their implementation of the current HIPAA compliant version of the accredited standards committee (ASC) X12N 276/277 health care claim status request and response format as established in the 004010X093 Implementation Guide (IG). In order to implement the HIPAA administrative simplification provisions, the 276/277 has been named under part 162 of title 45 of the Code of Federal Regulations as the electronic data interchange (EDI) standard for Health Care Claim Status Request/Response. All other EDI formats for health care claims status request and response become obsolete October 16, 2003.

The current HIPAA compliant version of the implementation guide for the 276/277 standard may be found at the following website: http://www.wpc-edi.com/hipaa/HIPAA_40.asp. The 276/277 is a "paired" transaction (the 276 is an in-bound claim status request and the 277 is on outbound claims status response).

20.1 - Transmission Requirements

(Rev. 1, 10-01-03)

Carriers, DMERCs and intermediaries (hereafter called contractors) may continue to operate automated response unit (ARU) capability for providers to request and receive claim status information. ARUs are not considered EDI and are not affected by the HIPAA requirements. Nor do they impact response time requirements for the standard transactions implemented under HIPAA.

20.1.1 - Batch Transactions

(Rev. 1, 10-01-03)

Contractors must be able to accept the current ANSI X12N 276 Health Care Claim Status Request Response version 4010 in batch mode, and respond via the ANSI X12N 277 Health Care Claim Status Response version 4010 in batch mode. If a contractor currently supports batch capability in any EDI batch format for providers to request claim status, the response time for issuance of a 277 transaction in response to receipt of a valid 276 must be as fast as or faster than the current batch claim status response time. The 277 response is issued within one business day of receipt of a valid 276 inquiry.

20.1.2 - Online Direct Data Entry (DDE)

(Rev. 1, 10-01-03)

HIPAA uses the term "direct data entry" generically to refer to a type of functionality operated by many different payers under a variety of titles. Within this instruction, the acronym DDE is being used to refer to any type of direct data entry system maintained by contractors, or shared system maintainers, including intermediary DDE or equivalent functionality that may have a different title. Although DDE operates online, DDE does not typically operate on a detailed inquiry and response basis. For claim status purposes, data is maintained within an interactive database that providers may access to view screens containing a wide variety of information on their claims. A provider accesses that data by furnishing certain identifying data for security purposes to establish their right to read the data and to specify those claim records the provider wishes to review.

The information in this database for specific claims or providers is initiated when a provider enters claim data, and is then updated by a contractor to include subsequent actions taken that affect that claim. DDE was specifically permitted to continue in the HIPAA initial transactions final rule (45 CFR 162.923), with the stipulation that direct data entry is subject to "…the applicable data content and data condition requirements of the standard when conducting the transaction. The health care provider is not required to use the format requirements of the standard."

Data content conformity means that the same information permitted or required by the 277 implementation guide must be reported in the claims status screens (the DDE outbound). The DDE outbound may not report a data element for claim status purposes that is not included in the 277, exceeds the maximum length of the data element in the 277, does not meet the minimum length for the data element in the 277, or that does not meet the 277 requirement that the data element be numeric, alpha-numeric, an amount, or meet another characteristic as specified in the 277. On the inbound, the DDE system can require less information than the 276, but not more. The inquirer is not required to furnish information in the DDE inquiry that is available by other means to the contractor. Any data element keyed in a DDE system must conform to the requirements. ANSI X12N standard implementation guides include data element length and characteristics in their definition of data attributes.

Conformity does not mean that a DDE screen that includes claim status information must display each of the data qualifiers or other means of data identification contained in the 277 implementation guide. DDE screens typically identify, explicitly or by context, the type of information being reported in a field, e.g., would identify if a number represents a HCPCS, health insurance claim number, amount, grams, date of birth, etc. DDE screens would not be expected to use a qualifier contained in the 277 to identify data type if that is otherwise evident in the design or content of the DDE screen.

Shared system maintainers must map the DDE claim status data elements to the 276/277 implementation guide to determine if the DDE claim status data elements meet the conformity requirements above. If needed, changes must be made to enable contractor DDE claim status data elements to conform.

If a contractor continues to support DDE, it must be offered in addition to batch 276/277, but the contractor must take one of two approaches to assure their claim status data content conforms to the requirements:

1. Eliminate claim status data elements from the DDE screens, unless those data elements are also needed for a purpose other than claim status. For example, if a data element is needed in a DDE screen for claim entry or claim correction, and it is also used to help determine claim status, retain the data element so it can continue to be used for claim entry or correction. If a data element is used solely for claim status, and is not essential for an alternate purpose, eliminate it; or

2. If a contractor elects to continue to display claim status-specific data elements in their DDE screens, those data elements must at a minimum contain/report data that conforms to:

    - All required and applicable conditional data elements for those segments in the 277; and

    - Data content as specified for those data elements in the 277, as applicable, including compliance with the data attributes for those data elements as defined in the 277 implementation guide.

Preliminary feedback from contractors suggests that existing DDE screens used for Medicare may already conform to the 277 implementation guide requirements, but data element mapping is required to verify. For example, since industry input was used to develop the 277 implementation guide as well as, presumably the data elements for claim status currently furnished via DDE, it is unlikely that DDE screen field sizes would be larger than the 277 maximum length or shorter than the 277 minimum length. It is also unlikely that a DDE screen would contain a data element considered important for claim status that is not included in the 277, or vice versa.

If a shared system maintainer determines that DDE screen changes are required, the maintainer in conjunction with its users must determine if it would be cost effective to modify the DDE screens to conform to the 277 implementation guide. If not cost effective, the maintainer must eliminate the claim status-only data elements from the DDE screens and require the contractors to use the batch 276/277, an ARU, and/or other non-EDI means to obtain claim status information.

If retention is cost effective, the maintainer must modify these screens as necessary to assure that providers are able to access all applicable data content available in the 277. The DDE screens must be able to furnish providers information that conforms to the data that would have been issued to the provider in a 277. See above for the discussion of conformity.

20.1.3 - Interactive/Online (Non-DDE)

(Rev. 1, 10-01-03)

Contractors are not required to accept a 276 query or respond with a 277 in an interactive, online mode if they do not already do so. If contractors do support the 276/277 in an interactive online mode, it must be offered in addition to batch 276/277. If they currently support the interactive/online (non-DDE) functionality, using the 276/277 version 3070 or any other direct claim status query and response EDI (non-DDE) format, they have the option to either:

- Terminate that support effective October 2003; or

- If they elect to continue that service beyond the end of September 2003, they must accept version 276inquiries and respond in the 277 format in an interactive online mode. Contractors may not continue to operate any other format or version for interactive, online (non-DDE) requests/responses for claim status information. Response time for issuance of data in the 277 format in response to receipt of a valid 276 must be as fast or faster as the interactive, online response time for claim status information prior to the contractor’s implementation of version 4010.

20.2 - Summary of the 276/277 Process for Carriers, DMERCs and Intermediaries

(Rev. 1, 10-01-03)

A. The contractor’s translator must perform interchange control and syntax edits on the submitted 276 data at the ANSI X12N standard level, generate a TA1 (or equivalent local reject report) in batch (or interactive mode if supported) if an interchange control error was detected, and generate a 997 in batch (or interactive mode if supported) if a syntax error is detected. In the absence of any interchange control or syntax error, a 997 is issued in the batch mode only, to confirm receipt of a 276 received via batch. Due to the quick response time for interactive, online transactions, a 997 is not issued to confirm receipt of a valid transaction; the 277 response itself signifies receipt of a valid 276. See §20.4 for additional translation requirements. Translation does not apply to DDE screens.

A TA1 (or local reject report) and 997 issued for a 276 submitted in a batch must be issued within 1 business day of receipt of the 276. A TA1 (or local reject report) or 997 for a 276 submitted in an interactive, online mode must be issued as quickly as the 277 would have been issued had the 276 been valid. If a contractor supported interactive, online access to claim status information for providers prior to implementation of the HIPAA compliant version of the 276/277, the HIPAA compliant version of the 277 TA1 (or local reject report) and 997 response time must be as fast or faster than the pre-version response time for this information. Each contractor must include its anticipated response times for the modes of 276/277 supported in their trading partner agreement. The error report should be made available as quickly as the 277 response would have been (had it been error free) whether the response is the TA1, 997 or the shared system generated error report.

The contractor's translator maps the inbound 276 data that have passed the interchange control and syntax edits to the 276 flat file, and forwards the data in the flat file format to the shared system within 1 business day of receipt of a valid 276.

B. The shared system must include edits to verify that the submitted 276 data complies with IG and Medicare requirements. If edits are failed, the shared system must generate an edit report following the model established for IG and Medicare program edit reporting for the HIPAA compliant version of the ANSI X12N 837 implementation. The edit report must include any reason(s) for the rejection in a concise but explicit manner that can be understood by provider staff as well as contractor staff. Contractors will forward the edit messages to submitters for correction of the edit condition. The shared system must generate these edit reports within 1 business day.

The IG edits must be performed as defined in the IG segment and data element notes, data element attributes, conditions of use, and overall guiding principals for use of the standards as contained in the introduction section and addenda to the IG. The Medicare program edits must be performed as required by current Medicare program instructions.

C. The shared system either:

- Stores any 276 data elements required for preparation of a compliant 277 response that are either not retained in the Medicare core system, or exceed the size limits for that type of data in the Medicare core system in a temporary file; or

- Uses an alternate method if less costly for that individual shared system but still compliant with the 277 IG requirements to complete a compliant 277 in response to that 276.

These requirements are implement without changing the core system or using a repository to store additional information. However, if the carrier analysis shows it would be more efficient to do either one, the carrier may do so.

D. The shared system searches the claims processing database for the information requested in the 276 and creates a flat file response that is returned to the contractor. (The shared systems maintainers in consultation with their users must develop minimum match criteria for the 276.)

E. The contractor translates the flat file data into the HIPAA compliant version of the 277 format and forwards the 277 to the provider.

20.3 - Flat Files

(Rev. 1, 10-01-03)

The CMS developed flat files that maintainers and contractors may use. The files are available in two formats - a single file containing both 276 and 277 data elements and separate files for each. Maintainers and their users should select which format they will use. The flat files provide for a one to one correlation between the core system data elements and the 276/277 data elements, and functions as a cross check to assure that necessary 276 data is submitted to the shared system and required 277 data can be extracted from the shared system.

Contractors must be able to accept a 276 transaction that complies with the HIPAA compliant version of the IG at the front-end and translate that data into the established flat file format for use by the shared system. Contractors must also be able to accept a flat file formatted feed from their shared system and create a compliant outbound 277.

Access the 276/277 flat files at the following website: http://cms.hhs.gov/providers/edi/hipaadoc.asp. The flat file format is a self-extracting compressed Excel spreadsheet.

20.4 - Translation Requirements

(Rev. 1, 10-01-03)

The translation software contractors previously obtained for implementation of HIPAA compliant version of the ANSI X12N 837 and 835 transactions must also be capable of translation of 276 and 277 data. A contractor translator is required to validate that the 276 and 277 meet the ANSI X12N interchange control and syntax requirements contained in the HIPAA compliant version of the 276/277 . Implementation guide and Medicare program edits are shared system, rather than translator, responsibility.

Contractors must accept the basic character set on an inbound ANSI X12N 276, plus lower case and the @ sign which are part of the extended character set. Refer to Appendix A, page A2 of the implementation guide for a description of the basic character set. The carrier translator may reject an interchange that contains any other characters submitted from the extended character set.

Contractor translators are to edit the envelope segments (ISA, GS, ST, SE, GE, and IEA) in order that the translation process can immediately reject an interchange, functional group, or transaction set not having met the requirements contained in the specific structure that could cause software failure when mapping to the ANSI X12N-based flat file. Contractors are not required to accept multiple functional groups (GS/GE) within one interchange.

A contractor's overall translation process must also:

- Convert lower case to upper case;
- Pass all spaces (default values) to the 276 flat file for fields that are not present on the inbound ANSI X12N 276. Do not generate a record on the 276 flat file if the corresponding segment is not present on the inbound ANSI X12N 276;
- Map "Not Used" data elements based upon that segment's definition, i.e., if a data element is never used, do not map it. However, if a data element is "required" or "situational" in some segments but not used in others, then it must be mapped;
- Remove the hyphen from all range of dates with a qualifier of "RD8" when mapping to the ANSI X12N-based flat file; and
- Accept multiple interchange envelopes within a single transmission.

All decimal data elements are defined as "R." A contractor's translator must write these data elements to the X12-based flat file at their maximum field size, which will be initialized to spaces. Use the COBOL picture found under the IG data element name of the flat file to limit the size of the amounts. These positions are right justified and zero-filled. The translator is to convert signed values using the conversion table shown below. This value is to be placed in the last position of the COBOL-defined field length. The last position of maximum defined field length of the 276 flat file data element will be used as a placeholder to report an error code if an "R" defined data element exceeds the limitation that the Medicare core system is able to process.

The error code values are:

"X" = value exceeds maximum amount based on the COBOL picture,

"Y" = value exceeds maximum decimal places based on the COBOL picture, and

"b" blank will represent no error.

For example, a dollar amount with the implementation guide maximum of 18-digits would look like 12345678.90. The translator must map this amount to the X12-based flat file using the COBOL picture of S9(7)V99. The flat file amount will be

23456789{bbbbbbbbX. The "{" is the converted sign value for positive "0." The error switch value is "X" since this value exceeded the COBOL picture of S9(7)V99.

Conversion Table

1 = A	-1 = J
2 = B	-2 = K
3 = C	-3 = L
4 = D	-4 = M
5 = E	-5 = N
6 = F	-6 = O
7 = G	-7 = P
8 = H	-8 = Q
9 = I	-9 = R
0 = {	-0 = }

20.5 - Transmission Mode

(Rev. 1, 10-01-03)

The HIPAA compliant version of the 276/277 transaction is a variable-length record designed for wire transmission. The CMS requires that the contractor accept the inbound and transmit the outbound over a wire connection.

20.6 - Restriction and Controlling Access to Claims Status Information

(Rev. 1, 10-01-03)

Provide claims status information to providers, suppliers and their agents when an EDI Enrollment Form is on file for that entity, and to network service vendors if there is an EDI Enrollment Form and EDI Network Service Agreement on file. (See Medicare Claims Processing Manual, Chapter 24, EDI Support Requirements for instructions on the enrollment form and the EDI Network Service Agreement.)

20.7 - Health Care Claims Status Category Codes and Health Care Claim Status Codes for Use with the Health Care Claim Status Request and Response ASC X12N 276/277

(Rev. 96, 2-6-04)

PM AB-03-029

PM AB-03-131

Medicare carriers and intermediaries must periodically update their claims system with the most current health care claims status category codes and health care claim status codes for use with the Health Care Claim Status Request and Response ASC X12N 276/277. The most current codes can be found at http://www.wpc-edi.com/codes/Codes.asp

Under the Health Insurance Portability and Accountability Act (HIPAA), all payers must use health care claims status category codes and health care claim status codes approved by the Health Care Code Maintenance Committee. At each X12 trimester meeting (generally held the months of February, June and October) the Committee may update the claims status category codes and health care claim status codes. Included in the code list are specific details such as the date when a code was added, changed or deleted.

By July 1, 2003, Medicare carriers and intermediaries were to have all applicable code changes and new codes that were posted to that Web site as of March 31, 2003, for use in production. The HCFA Part B Standard System (HPBSS) and its carriers were exempt from that requirement until carriers transitioned to the Multi-Carrier System (MCS).

By July 1, 2003, Medicare carriers and intermediaries were to have begun providing information in a regularly scheduled provider news bulletin regarding the implementation (and subsequent updates) to the claims status category codes and health care claim status codes for use with the Health Care Claim Status Request and Response, ASC X12N 276/277.

By September 1, 2003, Medicare carriers and intermediaries were to have all applicable code changes and new codes that were posted to the Web site with the "new as of February 03" designation and prior dates for use in production. They were not to update their system to include codes that were dated post-February 2003 until instructed. Medicare carriers and intermediaries were further instructed that if a code does not apply to Medicare, they were not required to accommodate it in their adjudication system nor in their 277 responses. If a Medicare carrier's or intermediary's adjudication system did not currently support the level of detail in any code, they were not required to accommodate the code in their system.

By September 1, 2003, Medicare carriers and intermediaries were to have informed providers/submitters of any new codes providers could see in 277 responses. Options for getting that message out included provider bulletins, educational articles, provider outreach presentations or electronic mail/web page/electronic bulletin board. Medicare carriers and intermediaries were to choose from any of these options (as well as others) to reach their provider/submitter audience by the most effective and efficient means timed with their system's availability of the codes to their providers/submitters.

By July 1, 2004, Medicare carriers and intermediaries are to have all applicable code changes and new codes that are posted to the Web site with the "new as of September 03" designation and prior dates for use in production. They are not to update their system to include codes that are dated post-September 2003 until instructed. If a code does not apply to Medicare, they are not required to accommodate it in their adjudication system nor in their 277 responses. If a Medicare carrier's or intermediary's adjudication system does not currently support the level of detail in any code, they need not accommodate the code. If providers are impacted by the July 2004 update, Medicare carriers and intermediaries shall inform affected provider communities by posting either a summary or relevant portions of this instruction on their websites within two weeks of the issuance date of this instruction. In addition, this same information shall be published in the next regularly scheduled Medicare carrier or intermediary bulletin. If a Medicare carrier or intermediary has a listserv that targets the affected provider communities, they must use it to notify those communities about this update.

CMS will issue instructions through the Change Request process regarding future changes to the codes. Contractor and shared systems changes will be made as necessary, as part of a routine release to reflect applicable changes such as retirement of previously used codes or newly created codes that may impact Medicare.

30 - Furnishing Claims Information to Complementary Insurers Under HIPAA

(Rev. 1, 10-01-03)

B-00-68

See Chapter 28 for general requirements for providing information to complementary insurers.

The Health Insurance Portability and Accountability Act (HIPAA) requires that Medicare, and all other health insurance payers in the United States, comply with the EDI standards for health care as established by the Secretary of Health and Human Services. The ANSI X12N 837 implementation guides for each transaction are available electronically at http://www.wpc-edi.com/hipaa/HIPAA_40.asp.

Transfer of payment information from a contractor to a billing service that submits assigned claims on behalf of a physician or supplier has been established as a "routine use," as provided for in the Privacy Act. Therefore, no special beneficiary signature requirements are needed to cover this transfer of payment information.

EDI submitters may send an inbound ANSI X12N 837 transaction that contains all data possible, and contractors must be able to accept it at their front end; however, they need not process non-Medicare information. They must retain the original inbound ANSI X12N 837 data in order to transmit a fully HIPAA-compliant outbound ANSI X12N 837 COB to their COB trading partners. This data must be stored in a repository file built by their shared system prior to entering their shared system's main processing system. The data in the repository file must be retrieved at the back end, along with data required for Medicare, to build a HIPAA-compliant outbound ANSI X12N 837 COB transaction. The ANSI X12N flat file accommodates COB data. In addition, contractors' direct data entry (DDE) screens must also be modified to collect all required data. The ANSI X12N format and data content requirements pertain to the DDE output if it is held outside a contractor's system and transmitted later. If the DDE output is entered directly into their system, only the data content requirements of the standard must be met.

Contractors and shared systems maintainers may use an alternate format for internal systems programming as long as incoming and outgoing transactions are translated to fully comply with the HIPAA requirements.

40 - ANSI X12N 278 - Electronic Referral Certification and Authorization

(Rev. 1, 10-01-03)

PM - B-02-53 (CR 2276)

Under the terms of the Health Insurance Portability and Accountability Act (HIPAA), the Secretary of Health and Human Services has established the Accredited Standards Committee (ASC) X12N (Insurance Standards Subcommittee) 278 (Health Care Services Review--Request for Review and Response) implementation guide (IG) as the national standard for electronic transmission of Referral Certification requests and Authorization responses. This standard must be used by all health care plans, including Medicare's durable medical equipment regional carriers (DMERCs) that conduct Referral Certification and Authorization. DMERCs and their shared system maintainer must complete implementation of the X12N 278 version 4010 by October 16, 2003, to meet the requirements of the administrative simplification provisions of HIPAA.

The IG can be downloaded at www.wpc-edi.com/hipaa. The shared system maintainer must develop a flat file that includes all required and applicable situational data elements as established in the IG, and that complies with the data content length and other data attributes established in that IG. The shared system maintainer must also develop a map between that flat file and the X12N 278 segments and data elements for use during translation of data between the flat file and the X12N 278 formats.

The X12N 278 implementation requirement applies to the DMERCs and their shared system maintainer only for Medicare fee-for-services purposes. Other shared systems and carriers do not conduct prior authorization.

50 - Related Internet Files Routinely Updated by CMS

(Rev. 1, 10-01-03)

The CMS correspondence, program memoranda, and flat files related to HIPAA are located at: http://cms.hhs.gov/providers/edi/hipaadoc.asp.