Program Memorandum Intermediaries/Carriers

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

Transmittal AB-02-171 **Date: NOVEMBER 25, 2002**

CHANGE REQUEST 2452

SUBJECT: X12N Health Care Eligibility Benefit Inquiry/Response (270/271) Transaction Security and Connectivity Instructions

Background

This Program Memorandum (PM) provides additional instructions for intermediaries and carriers, durable medical equipment regional carriers (DMERCs) herein referred to as "contractors", claims processing data centers (DCs), and their respective standard systems and the common working file (CWF) on Medicare requirements for connecting providers/vendors to DCs to request and receive eligibility information. Intermediaries should refer to Transmittal Nos. A-02-013 dated February 8, 2002, A-02-029 dated April 17, 2002 and A-02-065 dated July 24, 2002, for initial eligibility implementation instructions. Carriers should refer to Transmittal No. B-02-051, Change Request 2223, dated July 31, 2002, for the initial eligibility implementation instructions.

Within this PM the term "provider/vendor" or the term "provider" or "vendor" used alone refers to the actual covered entity who will submit a 270 transaction in order to receive a 271 response.

We expect most providers to use AT&T, CMS's current vendor for the Medicare Data Communications Network (MDCN), to obtain access to eligibility information. This PM contains instructions regarding how this transaction will be implemented, and explains the responsibility each party will have in order to use this transaction. Providers/vendors will connect to their respective data center in order to send a 270 transaction and receive back a 271 response. Specific instructions pertaining to this process are described in sections C-F of this PM.

If a contractor already has a private network, i.e., IVANS, AT&T, etc., that it uses to connect providers to the Medicare claims environment, then the contractor may add providers to that network.

A. Specific Instructions for Intermediaries

Intermediaries who have already established an LU6.2 interface may use LU6.2 to connect to the data center to gain access to the CWF module through the CICS region. If you have not already established an LU6.2 interface for connectivity you should not do so. All intermediaries (with and without LU6.2) should advise providers and vendors about the option of using TCP/IP for connecting to the data center as described in sections C and D of this PM. Intermediaries should advise providers/vendors to use the procedures for obtaining connectivity to the data center as described in section B and C of this PM.

B. Intermediary and Carrier Responsibilities

1. Contractors must establish a contact person at each site that will be responsible for handling the connection process for providers/vendors, and submit the name(s) to MDCN@cms.hhs.gov and e-mail a copy to ksimmons@cms.hhs.gov and to an appropriate contact person at each of your data centers for coordination purposes by December 13, 2002. The contractor should also provide the name of the data center they use, and the IP address that will be used for this purpose.

2. Contractors must distribute basic information related to the options for connectivity to each provider/vendor or other designated provider agent that has indicated a desire to use this method to obtain eligibility data. The contractor should obtain information about the hours of operation for eligibility access from each data center. Contractors are responsible for notifying providers/vendors about all of the network options available to connect to the data center. Each contractor is required to provide the name of the data center to which the provider/vendor will send the 270 transactions. Contractors must not encourage providers to use their existing network instead of using the MDCN connection to their data center. However, contractors may allow providers to use an existing network if one is available.

3. Contractors should inform providers and vendors that they may establish a direct bill sponsorship agreement with IVANs to obtain connectivity to the data center via the AT&T network. The contact person at each contractor will contact IVANS with a list of providers who intend to establish an agreement with IVANS.

4. Once a provider or vendor has expressed interest in obtaining connectivity, contractors must send a copy of the IVANS Communication Service Agreement for AT&T services to the provider, as well as other pertinent information needed to connect to the network. The actual Agreement, proposed costs, and help desk information will be distributed to contractors in a subsequent instruction. 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. However, contractors will have a sponsorship agreement with IVANS and will provide IVANS with a list of legitimate providers/vendors who have requested an IVANs Agreement. A copy of this Agreement will be provided in a subsequent PM. IVANS will provide a list of connected providers/vendors to each contractor once the actual connection has been established. The list will contain the AT&T user IDs for each provider/vendor.

5. After the provider/vendor signs the Agreement and the contractor approves the provider/vendor's access to IVANS, IVANS will then assign an account number and will send the signed Agreement to AT&T. AT&T will then establish an account for the provider and assign an AT&T network user ID and password to the provider/vendor. The contractor will contact the data center to get an IP address and port number for that provider/vendor in order to connect to the AT&T network. The contractor will notify the provider of the address to use. The data center will also assign a user ID and password for each provider/vendor to allow access to the data center's Customer Information Control Standard (CICS) region.

6. The data center must run the CWF shared software "One-Timers", e.g., special JCL job provided by the CWF maintainer, to create the security and audit files for the contractor's CICS region. The contractor must populate the CWF security file with data for each provider and vendor that the contractor approves to receive eligibility information. This file resides at the contractor's claims processing data center. The contractor will also need to update and maintain these files on an ongoing basis.

7. If the contractor currently offers eligibility information via direct data entry (DDE), providers/vendors may continue to use DDE. The FISS and APASS standard systems maintainers are not making any changes to DDE at this time. MCS and ViPs have made changes per CR2223. ViPs will implement the changes to DDE on January 6, 2003. VIPs carriers must notify their DDE users of the additional data elements that will be available as of January 6, 2003. MCS will develop a bridge between the Professional Provider Telecommunications Network (PPTN) eligibility inquiry option to the new CWF eligibility file/screens (the 270/271 module). These changes will be implemented on January 6, 2003. However, because the security portion of the CWF software will not be ready until the April release, MCS DDE users will not have the ability to query for eligibility until April 1, 2003. MCS carriers must notify their DDE users that eligibility queries via DDE will not be available from January 6, 2003 to April 1, 2003. These DDE users should also be informed that the available data set will be expanded April 1.

C. Provider and Clearinghouse Outreach-What Contractors Must Tell Providers/Vendors

Contractors must provide information regarding the implementation of the ANSI X12N 4010 270/271 to their providers, third-party provider billing services, provider clearinghouses, and

vendors through a regularly scheduled news bulletin and on the contractor's Web site. Contractors must also inform providers, billing services, provider clearinghouses, and vendors that if they want to send and receive the 270/271, they must contact their contractor to establish connectivity for real-time 270/271 eligibility/ benefit inquiry capability.

EDI requests for eligibility data must be submitted via a version 4010 270 eligibility query effective October 2003, and each valid 270 will be issued a version 4010 271 response. Prior eligibility formats will be discontinued effective October, 2003, although the information will still be available via DDE, ARU, or other *non-EDI* method a contractor has elected to support.

D. Provider/Vendor Responsibilities

Queries to CWF

1. It is the provider's/vendor's responsibility to develop a client TCPIP (streaming socket) program to connect to the data center's IP address. The TCPIP socket program will use the Client-Listener-Child-Server model. If a provider requires assistance to install the client TCP/IP (streaming socket) the provider may employ a software vendor to assist the organization to establish this connection. The provider will first transmit transaction "ELGV" for Part B eligibility or "ELGU" for Part A eligibility to initiate the host server listener program. Samples of client TCPIP programming can be found at the following Web sites:

   publibfp.boulder.ibm.com/cgibin/bookmgr/LIBRARY Manual CICS TCPIP Sockets Interface Guide, Document Number SC31-8518, and www.msdn.microsoft.com/library/default.asp, for sample Microsoft Winsock Applications.

Providers/Vendors with current LU 6.2 connectivity will need to modify the following connection identifiers and notify their Data Center. 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	

2. Since the data center is required to perform a user ID and password verification prior to processing a compliant X12N 4010 270 transaction, the data center user ID and password must be prefixed with each 270 request to allow the data center to authenticate each user's access to the CICS region. Data can be in upper case or lower-case. Providers/vendors should contact AT&T if they have problems with telecommunications connectivity to the data center. Furthermore, providers must contact their carrier if they are terminated from their AT&T contract for any reason at any time.

The format for the 270 transaction security prefix is as follows:

Data Element	Description	Bytes (66)	Content
Transaction	Transaction ID to	04 Characters	"ELGV" for TCP/IP start 270 Processing
Transaction Reference No.	Unique record identifier	30 Characters	Record Identifier
User ID	User ID provided by the data center to the provider	08 Characters	Provider USERID

Password	Password provided by data center to the provider	08 Characters	Current Password
Password1	New password changed by user	08 Characters	New Password
Password2	New password verification	08 Characters	New Password
270 data follows	ISA and other segments		

3. Below is the description of the security prefix layout data elements:

   - The transaction ID 'ELGV' identifies the record as a Part B Eligibility transaction via TCP/IP. The transaction ID 'ELGU' identifies the record as a Part A Eligibility transaction via TCP/IP and the transaction ID 'ELGL' identifies the record as a Part A Eligibility transaction via LU6.2.

   - Providers/vendors that process asynchronous eligibility transactions may utilize the Transaction Reference No. data element to uniquely identify each 270 query. The Transaction Reference No. will allow the organization to match the CWF response to the corresponding 270 query in the situation where CWF was unable to read/translate the incoming 270.

   - Providers will be required to send User ID and password fields with every 270 transaction. Providers will also be required to change passwords periodically. Providers should follow these steps to change passwords:

     To change the password, set the field *Password* to the old password. Then setting the fields *Password1* and *Password2* to the new password will reset the password.

4. Upon successful authentication, the subsequent 270 data will be sent to the CWF eligibility system.

5. At this time, CMS is only supporting on-line, real-time 270/271 transactions. However, providers have the option to configure their own software or use a vendor to set up what looks to the provider like a batch 270 transaction. The provider could also configure software to take the on-line 271 response from the data center and make it look to the provider like a batch reply.

Responses from CWF

6. CWF will return a 271/997/TA1 prefixed with the following proprietary record format. For all successful CWF responses, either a 271, 997 or a TA1 will follow the prefix. The layout for the 271/997/TA1 can be found in the version 004010 Implementation Guide for 270/271 at www.wpc-edi.com/HIPAA. This proprietary format is necessary to return information for situations when Provider login has failed the Data Center User Authentication process; or when CWF was unable to read/translate the 270 data due to system problems. Error messages relating to data center security authentication and System abends will be returned in the CWF Proprietary prefix layout in *Message Text* with the appropriate settings of *Response-code* and *Message-code*. The CWF maintainer will provide each data center with their hours of operation.

Format for the CWF Response (271/997/TA1) prefix is as follows:

Data Element	**Description**	**Bytes(128)**	**Content**
Transaction	Transaction ID	04 Characters	"ELGV" – Part B TCP/IP "ELGU" – Part A TCP/IP "ELGL" – Part A LU6.2

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 from CWF	02 Characters	Return Codes 'A' – System Abends 'E ' – CWF Errors 'F ' – Password Verification Failure 'T ' – CWF Timeout 'S ' – Successful
Message Code	Error Code from CWF	08 Characters	EIBRESP and EIBRESP2
Message Text	Error Description	70 Characters	Error Description

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

   - The transaction ID 'ELGV' identifies the record as a Part B Eligibility response via TCP/IP. The transaction ID 'ELGU' identifies the record as a Part A Eligibility response via TCP/IP and the transaction ID 'ELGL' identifies the record as a Part A Eligibility response via LU6.2.

   - 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.

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

   - 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.

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

8. 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.

9. 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. CWFM will add the carrier or intermediary number to the audit file. This new field will follow the transactions information status field.

The implementation date for the aforementioned changes for the CWF maintainer is January 2003.

E. Data Center TCP/IP Installation and Connectivity

Each data center must inform contractors about the hours of operation for access to eligibility information. The hours should be the same for each group of contractors. Each data center should establish hours of operation for each customer that will not cause a cost increase to the respective customer. For some, this may be 8:00 a.m. to 8:00 p.m.; for others the hours of operation could be much longer.

1. Each data center must install TCP/IP at the data center and CICS TCP/IP socket interface in the CICS region where the CWF software resides. Data centers can refer to the following suggested procedures to install TCP/IP:

   - Data centers may refer to IBM Book **TCPIP V3R2 for MVS: CICS TCPIP Socket Interface Guide, Document Number: SC31-7131-03.** Chapters one and two have instructions on setting up and configuring CICS TCPIP. This book also covers the installation of enhanced native TCPIP 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.

   - Install information can also be found in Online Library Omnibus Edition, OS/390 Collection (SK2T-6700) and the IBM Intranet at www.publibfp.boulder.ibm.com/cgi-bin/bookmgr/LIBRARY.

2. The data center must establish IP addresses and port numbers for providers upon carrier's approval of the provider. The data center must establish one port for the socket interface.

3. The data center must establish CICS user ID and password for the provider to allow the provider access to the carrier CICS region to perform online 270/271.

4. The data centers will use one of the security packages for user authentication. The CWF software security application will only validate against the security packages defined as follows:

   - RACF;
   - ACF2; or
   - TOP SECRET.

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

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

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

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

F. CWF Application Software Security

1. The CWF shared software will provide a back end interface to validate the CICS User ID and password prior to reading the 270. The module ELGXSTTC will handle the interface and security validation of the TCPIP transmission.

2. The CWF maintainer (CWFM) has developed CWF software application security screens for carriers to enter provider and submitter information.

3. The CWFM has developed CWF software application to perform security checking for all 270 requests.

G. Testing

Maintainers must coordinate with their data centers to test the security and audit file requirements with the CWF beta site. Contractors should coordinate and make sure that testing of the security and

audit file requirements are performed by the data center with their standard systems maintainers. However, contractors will not be involved in the actual test since the transaction is between the provider and the data center. Contractors will need to contact providers/vendors to set up the security aspect of the transaction. Testing with providers/vendors must be done between the data center and the provider/vendor. The provider may deal directly with the data center for connection issues, but contractors should be available to provide assistance if necessary.

Contractors and data centers should be ready for provider/vendor testing to begin by April 1, 2003.

H. Help Desk Issues

Contractors should be prepared to provide overall support and technical guidance to providers regarding the generic layout of the 270/271 transaction set and the Medicare implementation guide requirements. However, issues related to provider connections to the data center will need to be addressed by IVANs.

I. Cost Issues

Since this PM contains the details of the security and connectivity requirements for this transaction, the October 15, 2002, deadline for submitting contractor supplemental budget request (SBRs) has been changed to December 20, 2002. Any data center costs should be included in the contractor SBRs. Data centers that are under direct contract with CMS should contact their project officer regarding funding issues if necessary.

J. Implementation Schedule

The *effective date* for this PM is January 1, 2003.

The *implementation date* for this PM is April 1, 2003.

The implementation dates are as follows:

- For CWF maintainer: January 1, 2003.
- For standard systems maintainers: April 1, 2003
- For data centers and carriers and intermediaries: April 1, 2003

This PM may be discarded after January 1, 2005.

Medicare contractor questions concerning this PM may be directed to Kathleen Simmons, 410-786-6157, or e-mail to ksimmons@cms.hhs.gov.

Any provider, clearinghouse, or vendor with questions related to this PM must contact their servicing Medicare contractor.