CHANGE REQUEST 2576

SUBJECT: 270/271 Implementation and Direct Date Entry (DDE) Eligibility

I. Background

This Program Memorandum (PM) provides instructions and replaces the following previously issued PMs in regard to X12 270/271 implementation under the Health Insurance Portability and Accountability Act (HIPAA): A-02-013 (CR2009), A-02-029 (CR2111), B-02-033 (CR2182), B-02-051 (CR2223), A-02-065 (CR2234), and AB-02-171 (CR2452). This PM applies to Intermediaries, Carriers, Durable Medical Equipment Regional Carriers (DMERCs), herein referred to as "contractors," claims processing Data Centers (DCs), their respective shared systems maintainers, and the Common Working File (CWF) maintainer. This PM includes the Medicare requirements for implementation of the X12N Health Care Eligibility Benefit Inquiry/Response transaction (270/271) version 4010A.1, as well as other requirements applying to eligibility queries and responses in general for Medicare. This PM contains a workflow for the overall eligibility inquiry and response process, and explains each impacted party's responsibility regarding access to Medicare beneficiary eligibility information. This PM and its attachments can be electronically retrieved at www.cms.hhs.gov/providers/edi/default.asp. The HPBSS system maintainer is not required to make these system changes. HPBSS carriers will not implement these changes until they transition to MCS.

II. Eligibility Queries Options and Workflow

The following provides a basic description of the process to be followed. To preserve continuity to the extent possible, the workflow is being printed separately from the supplemental information explaining requirements listed in the workflow (see attachment 3). Subsequent sections of this PM further explain the role of the various parties involved in the process. 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.

CMS-Pub. 60AB

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, 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 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 your 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 2 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 your 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 on-line 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 5 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 5 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.

III. Eligibility Query Types

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 X12 271 transaction.

The HIQA, HUQA, and/or HIQH will be terminated effective October 16, 2003. (For a complete description of definitions for the transactions, please go to the CWF Web site:

http://cms.csc.com/cwf/. CWF must be sent the beneficiary's health insurance claim number, the first 6 characters of the beneficiary's surname, the beneficiary's first initial, and date of birth to retrieve eligibility data for the beneficiary.

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 X12 270 version 4010A.1 by October 16, 2003. Real-time responses will be returned to the submitters in the X12 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 X12 270 version 4010A.1 by October 16, 2003. Real-time responses will be returned to the submitters in the X12 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 X12 270 version 4010A.1 and be real-

time. Medicare will return real-time responses in the X12 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 Medicare Carriers Manual Part 3 §3021, and Medicare Intermediary manual Part 3 §3601. 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 X12 270 version 4010A.1 format by October 16, 2003. Contractors will send real-time X12 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. ASC X12 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 will be posted to the following Web site: www.cms.hhs.gov/providers/edi/default.asp by March 28, 2003.

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. Co-insurance 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

IV. Intermediary and Carrier Responsibilities

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. 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.

IVANS 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 you have not yet received that information from IVANS or have not yet submitted a signed sponsorship agreement. (See workflow items 6 a, b, c.)

B. Contact your 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 your 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.)

C. Include information in your next regularly scheduled provider bulletin and on your 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. X12 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. X12 271 version 4010A.1 responses, or error reporting transactions including the 997, TA1, and your 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 you, 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 you 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: You 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 you to obtain further information or to arrange for IVANS connectivity.
18. Any other information you would consider 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. Submit a funding request as mentioned in 1.c of the workflow within three weeks of the issue date of this PM to your HIPAACCMS representative you're your electronic data interchange (EDI) CCMS representative. Send a copy to your regional CMS financial management representative, and to KSimmons@cms.hhs.gov. If you had submitted a funding request for eligibility costs prior to receipt of this PM that you consider to still be accurate, resubmit that request with a statement that it includes costs for the activities related to CR 2576.

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.

V. Data Center Responsibilities

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.

VI. Provider/Network Service Vendor's Responsibility
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 X12 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	08 Characters	New Password

changed by user

Password2   New password   08 Characters   New Password
verification

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	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	02Characters	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

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.

VII. Supplemental CWF Module Information

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:

The *effective date* for this PM is July 1, 2003, or as otherwise indicated within the body of the PM for certain tasks assigned in prior PMs.

The *implementation date* for this PM is July 1, 2003, or as otherwise indicated within the body of the PM for certain tasks assigned in prior PMs.

See section IV.D of this PM for funding request requirements.

This PM may be discarded after July 1, 2004.

If you have any questions, contact Shari Kosko at: 410-786-6159 or skosko@cms.hhs.gov

DRAFT   DRAFT   DRAFT
            DRAFT   DRAFT   DRAFT

SPONSORSHIP AGREEMENT

Agreement between *IVANS, Inc.*, 1455 East Putnam Avenue, Greenwich, CT   06870-1037 and_____
_____("Member", "You").

IVANS agrees to establish a Customer Direct Billing Program, billing monthly via Invoice, for users whom you wish to authorize for access to applications described below. The establishment of this account is governed by the following understanding:

1.   *IVANS* will require that each user whom You authorize sign a separate Communications Service Agreement.

2.   *IVANS* will bill your authorized users for *IVANS* services and be responsible for collection and credit risk for all network charges and service charges incurred by these authorized users.

3.   Network usage of Your authorized users will be subject to *IVANS'* standard subscriber discounts, applied individually to each user. The total of the usage of all Your authorized users in the Customer Direct Bill Program will, however, be aggregated with Your other *IVANS* accounts for the purpose of setting the discount level applicable to those other *IVANS* accounts.

4.   You will use reasonable efforts to cooperate with *IVANS* when collection or billing disputes arise on issues concerning access to or satisfaction with the application for which you are authorizing users.(???????)

5.   You will provide authorization for initial user setup for this program and at any time may direct *IVANS,* in writing, to discontinue services to any or all users. You may re-authorize users who had services discontinued for reasons other than non-payment or credit problems. *IVANS* will maintain final approval over the issuance of user ids.

6.   *IVANS* may discontinue access at any time to users who fail to pay required services fees and network charges. You may not re-authorize users who have had their access discontinued for failure to pay without *IVANS'* agreement.

7.   *IVANS* will publish changes in network usage charges and discounts to you and to authorized users with thirty days notice.

8.   *IVANS* will charge each user a Monthly Service Charge of $11.50. *IVANS* may subsequently change this fee with 60 days' notice to you and to affected users.

9.   *IVANS* reserves the right to discontinue this program upon 120 days' notice to you.

10.   You will maintain a designated contact person to coordinate program administration with *IVANS, Inc.* Registration Department. At *IVANS, Inc.* request, you will include *IVANS, Inc.* Registration Department on your mailing list for information which you distribute to authorized users concerning procedural or other application usage matters.

11.   Description of Application and Type of Users:

_____

_____

_____

_____

Agreed to and accepted:

IVANS, Inc
Member: _____

By_____
By_____
   (Authorized Signature)
   (Authorized Signature)

Name_____   Name_____
   (Type or Print)
                        (Type or Print)

Title_____
Title_____
   (Type or Print)
                        (Type or Print)

Date_____
Date_____
   (Type or Print)
                        (Type or Print)

IVANS, INC.
COMMUNICATIONS SERVICE AGREEMENT

Customer Name: _____

Address:_____

City:_____State:_____Zip:_____

Customer Contact:_____Title:_____

Phone:_____ Fax: _____

Billing Address:_____
(if different from above)
City:_____State:_____Zip:_____

Contact:_____Phone:_____
(if different from above)
E-Mail Address:_____ Number of Workstations: _____

Medicare Provider Number: _____

_____ ("Sponsor") has authorized you to use the *IVANS/AT&T* Network for access to certain services provided that you agree to pay *IVANS*' charges which will consist of:

Monthly Service Charge	$ 11.50
Secure IP Local Dial Access	$ 3.40 per hour
SNA Gateway Surcharge, if used	$ 0.90 per hour
Additional Charge For Fee 800# Service, if used	$ 5.50 per hour
Software Installation Assistance, if used	$ 25.00 per desktop

To access _____ Services, you will need to install the AT&T NetClient and Passport software. Please check which option you prefer:

(   ) Mail me the AT&T NetClient and Passport Software. Specify # copies needed ____ at $15.00 per CD-ROM.

(   ) I will download The AT&T NetClient and Passport software at no charge from the following sites:
For Passport Software: ftp://ftp.attglobal.net/pub/passport/win95   select the file >>>> pasydes.exe
For AT&T Netclient: ftp://ftp.attglobal.net/pub/client/win32/ncsetup.exe

You also agree that your access to the *IVANS/AT&T* Network Facility will be subject to the terms and conditions printed on the reverse side of this agreement. **If you are a tax-exempt entity, please see Section 4 on the reverse side.**

By: _____   Name: _____
            (Authorized Signature)   (Type or Print)

Title: _____   Date: _____
                 (Type or Print)

Mail or fax <u>both sides</u> of this completed agreement to:
IVANS,
Attention: Direct Bill Department
5405 Cypress Center Drive, Suite 150
Tampa, FL 33609-1022

Should you have any questions about this agreement or if you desire to contact *IVANS* for any reason please write: *IVANS, Inc.,* 5405 Cypress Center Drive, Tampa, FL 33609-1022, Attention: Direct Bill Department, or call IVANS Help Desk, 1-800-548-2675, choose option 3, choose option 1; Fax 813-282-7029.   .

IVANS, INC. COMMUNICATIONS SERVICE AGREEMENT

Under this Agreement, you, the Customer ("User"), may access the *IVANS* network on the following terms and conditions:

1.   **IVANS' SERVICE**: The service consists of access to the *IVANS* Network for the purpose of using communication, information, database or computing services authorized for you by an *IVANS*' Member or Subscriber Member ("Sponsor"). Use of these services is subject to this agreement and any supplemental operating terms and conditions including copyright and confidentiality notices published in connection with individual services, options or facilities. *IVANS*' may suspend your access to this service without notice at your Sponsor's direction or at *IVANS*' discretion in the event your Sponsor does not maintain its membership status in *IVANS*.

2.   **ACCESS TO NETWORK**: Access to the *IVANS* network will be provided on a schedule made available to User, but may be limited at the discretion of *IVANS* for emergency repairs or as a result of circumstances beyond *IVANS*' control.

3.   **CHARGES**: Use of services or products other than those shown on the first page of this Agreement will lead to additional charges based on *IVANS'* current rates for those services and products. *IVANS* reserves the right to modify charges effective thirty (30) days after notice to User. *IVANS* also reserves the right to add or withdraw products and services with notice to user. All charges are exclusive of federal, state or local sales, use, or personal property taxes or taxes of a similar nature. Any such taxes which may be applicable will be paid by User or by *IVANS* for User's account. User acknowledges and agrees that it shall be solely responsible for any long distance telephone charges necessary for access to the *IVANS* network. Termination or suspension of account for non-payment, and subsequent re-activation, may incur an additional charge.

4.   **TAX STATUS**. All charges are exclusive of federal, state or local sales, use, or personal property taxes or taxes of a similar nature that may apply to the Service. Any such applicable taxes will be paid by User or by *IVANS* for User's account. If User is a tax-exempt entity, a copy of the applicable state exemption certificates(s) must be provided to IVANS with this Agreement, or if no exemption certificate is available in User's state, a copy of the applicable Sales and Use Tax Exemptions and Exclusions Regulations for the State.

5.   **BILLING AND PAYMENTS**: Customer will be invoiced on a schedule established by *IVANS*, with payment due within 21 days of the date of invoice. If User learns or suspects that unauthorized use of this account is taking place, it must notify *IVANS* immediately and, in such event, *IVANS* will cancel User's password and provide User with a new one. Delinquent accounts are subject to interest charges of one and one-half (1½%) percent per month or the maximum limit allowable by law on the unpaid balance, whichever is less, plus all costs of collection, including reasonable attorney's fees. *IVANS* reserves the right to suspend service to a delinquent account without notice.

6.   **LIMITATION OF WARRANTY**: CUSTOMER EXPRESSLY AGREES THAT USE OF THE SERVICE AND MATERIAL THEREIN AND STORAGE OF INFORMATION WHICH APPEARS IN THE SERVICE IS AT CUSTOMER'S SOLE RISK. NEITHER *IVANS* NOR ANY OF ITS LICENSORS, SUPPLIERS, OR AGENTS WARRANTS THAT THE SERVICE WILL BE UNINTERRUPTED OR ERROR FREE; NOR IS ANY WARRANTY MADE AS TO THE RESULTS TO BE OBTAINED FROM USE OF THE SERVICE. THE SERVICE IS DISTRIBUTED ON AN "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE.

7.   **IVANS LIABILITY**: *IVANS* exclusive liability for any claim of any kind relating to this Agreement or to the products and services provided hereunder shall not exceed the fees paid for use of the services and *IVANS* liability shall terminate if no action is commenced within one year after a cause of action has occurred. IN NO EVENT SHALL *IVANS* BE LIABLE FOR SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES TO GOODS OR EQUIPMENT, LOST PROFITS, DOWNTIME COSTS, LABOR COSTS, OVERHEAD COSTS, CLAIMS OF CUSTOMERS OR CLIENTS OR USER, OR DELIVERY OF DATA CONTAINING INACCURACIES OR OMISSIONS THAT WERE PRESENT WHEN THE DATA WAS RECEIVED BY *IVANS*.

Some states do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

8.   **INDEMNIFICATIONS**: Customer shall indemnify and hold *IVANS* and its affiliates harmless from all claims made by Customer's employees, clients or customers or their employees, clients or customers.

9.   **TERM**: This agreement will remain in effect until written notice of termination for any reason is rendered by either party to the other. If dedicated lines, frame relay or similar products are in use, the Customer must provide sixty (60) days advance written notice of termination. Notwithstanding anything to the contrary, IVANS has the right to terminate this agreement if Customer files for bankruptcy.

10.   **ASSIGNMENT**: This Agreement may not be assigned by Customer without the prior written consent of *IVANS*.

11.   **GOVERNING LAW**: This Agreement is to be governed by and interpreted in accordance with the laws of the State of Connecticut.

12. If Customer is a corporation, partnership or other business entity, the individual agreeing to these terms has full authority and power to enter into this Agreement. No terms or conditions in any purchase order or other document shall supersede the terms of this Agreement.

IVANS, INC.
COMMUNICATIONS SERVICE AGREEMENT - LEASED LINE

Customer Name: _____

Address: _____

City: _____ State:_____Zip:_____

Customer Contact: _____ Title:_____

Phone: _____ Fax: _____

Billing Address _____
(if different from above)

City: _____ State: _____ Zip: _____

Contact: _____ Phone:_____
(if different from above)

E-Mail Address: __Medicare Provider Number:_____

IVANS is an industry association providing data networking solutions for our members in the health and insurance industries. Many of these products and services are delivered through *IVANS* partnership with the AT&T Global Network.

_____("Sponsor") has authorized you to use the *IVANS/AT&T* Network for **Leased Line access to the application** _____ provided that you agree to pay *IVANS*' charges for the AT&T Leased Line circuits identified below and detailed in the Leased Line Pricing Attachments, plus a monthly service fee for each IVANS invoice of $11.50. A deposit equal to one months' charge must be submitted with this Agreement. Please refer to the attachments for the appropriate monthly charge.

Line Speed Options

✓	Line Type	Pricing Attachment	9.6 kbps	19.2 kbps	56 kbps	128 kbps	256 kbps	384 kbps	512 kbps	768 kbps	1,024 kbps	T1, 1,544 kbps
	SNA Site Connection	I			N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	SNA Host Connection	II			N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
	FRAME RELAY SNA Only	III	N/A	N/A								
	FRAME RELAY IP Only	IV	N/A	N/A								
	FRAME RELAY SNA & IP	V	N/A	N/A								

You agree that your use of *IVANS* services and access to the *IVANS/AT&T* Network Facility will be subject to the terms and conditions of this Agreement. Additionally, You request that IVANS place the order for the Leased Line identified above and in the Leased Line Pricing Attachment, and order an account id. IVANS has the right to deny your application for service based on any credit investigation that IVANS shall, at its   discretion, initiate. **If you are a tax-exempt entity, please see Section 4 on the reverse side.**

Customer:
By_____Date_____
        (Authorized Signature)   (Type or Print)

Name and Title _____
                        (Type or Print)

Please mail this completed agreement and your one-month deposit check to: Leased Line Enrollment Coordinator, IVANS, Inc., 1455 East Putnam Avenue, Old Greenwich, CT 06870. For questions, please call our Tampa Customer Support Center at 800-548-2675. Thank you for your business and welcome to IVANS.

IVANS, INC. COMMUNICATIONS SERVICE AGREEMENT - LEASED LINE

Under this Agreement, you, the Customer ("User"), may access the *IVANS* network on the following terms and conditions:

1. **IVANS' SERVICE**: The service consists of Leased Line circuit access to the *IVANS/AT&T* Network for the purpose of using communication, information, database or computing services authorized for you by an *IVANS'* Member. ("Sponsor"). Use of these services is subject to this agreement and any supplemental operating terms and conditions including copyright and confidentiality notices published in connection with individual services, options or facilities. *IVANS'* may suspend your access to an *IVANS* Member at the direction of that *IVANS* Member without notice to you or at *IVANS'* discretion in the event your Sponsor(s) does not maintain its membership status in *IVANS*.

2. **ACCESS TO NETWORK**: Access to the *IVANS/AT&T* network may be limited at the discretion of *IVANS/AT&T* for emergency repairs, scheduled maintenance or as a result of circumstances beyond *IVANS*'' or AT&T's control.

3. **CHARGES**: The current *IVANS* charges for this service are provided to you with this agreement. *IVANS* reserves the right to modify charges effective thirty (30) days after notice to User. *IVANS* also reserves the right to add or withdraw products and services with notice to user. User acknowledges and agrees that it shall be solely responsible for any long distance telephone charges necessary for access to the *IVANS* network. Termination or suspension of account for non-payment, and subsequent re-activation, may incur an additional charge.

4. **TAX STATUS**. All charges are exclusive of federal, state or local sales, use, or personal property taxes or taxes of a similar nature that may apply to the Service. Any such applicable taxes will be paid by User or by *IVANS* for User's account. If User is a tax-exempt entity, a copy of the applicable state exemption certificates(s) must be provided to IVANS with this Agreement, or if no exemption certificate is available in User's state, a copy of the applicable Sales and Use Tax Exemptions and Exclusions Regulations for the State.

5. **HEALTH PROVIDER MEMBERSHIP.** By signing this agreement you are requesting access to the Sponsor's application. If you desire access to multiple payors'/companies' applications you must become an IVANS Health Provider member. Please contact the IVANS Healthcare Account Manager, 800-548-2675, for information.

6. **BILLING AND PAYMENTS**: Customer will be invoiced on a schedule established by *IVANS*, with payment due within 21 days of the date of invoice. Delinquent accounts are subject to interest charges of one and one-half (1 %) percent per month or the maximum limit allowable by law on the unpaid balance, whichever is less, plus all costs of collection, including reasonable attorney's fees

7. **LIMITATION OF WARRANTY**: CUSTOMER EXPRESSLY AGREES THAT USE OF THE SERVICE AND MATERIAL THEREIN AND STORAGE OF INFORMATION THAT APPEARS IN THE SERVICE IS AT CUSTOMER'S SOLE RISK. NEITHER *IVANS* NOR ANY OF ITS LICENSORS, SUPPLIERS, OR AGENTS WARRANTS THAT THE SERVICE WILL BE UNINTERRUPTED OR ERROR FREE; NOR IS ANY WARRANTY MADE AS TO THE RESULTS TO BE OBTAINED FROM USE OF THE SERVICE. THE SERVICE IS DISTRIBUTED ON AN "AS IS" BASIS WITHOUT WARRANTIES OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE.

8. *IVANS* **LIABILITY**: *IVANS* exclusive liability for any claim of any kind relating to this Agreement or to the products and services provided hereunder shall not exceed the fees paid for use of the services and *IVANS* liability shall terminate if no action is commenced within one year after a cause of action has occurred. IN NO EVENT SHALL *IVANS* BE LIABLE FOR SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES, INCLUDING WITHOUT LIMITATION DAMAGES TO GOODS OR EQUIPMENT, LOST PROFITS, DOWNTIME COSTS, LABOR COSTS, OVERHEAD COSTS, CLAIMS OF CUSTOMERS OR CLIENTS OR USER, OR DELIVERY OF DATA CONTAINING INACCURACIES OR OMISSIONS THAT WERE PRESENT WHEN THE DATA WAS RECEIVED BY *IVANS*.

   > Some states do not allow the limitation or exclusion of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

9. **INDEMNIFICATIONS**: Customer shall indemnify and hold *IVANS* and its affiliates harmless from all claims made by Customer's employees, clients or customers or their employees, clients or customers.

10. **TERM AND TERMINATION**: This agreement will remain in effect until written notice of termination for any reason is rendered by either party to the other. The Customer must provide IVANS with sixty (60) days' advance written notice of termination, unless such termination is the result of a price change under Section 3, in which event Customer may terminate this Agreement with thirty (30) days' advance written notice. *IVANS* reserves the right to suspend service to delinquent accounts without notice. Notwithstanding anything to the contrary, IVANS has the right to terminate this agreement if Customer files for bankruptcy.

11. **ASSIGNMENT**: This Agreement may not be assigned by Customer without the prior written consent of *IVANS*.

12. **GOVERNING LAW**: This Agreement is to be governed by and interpreted in accordance with the laws of the State of Connecticut.

13. Neither *IVANS* nor AT&T makes any representation as to the quality of the information relayed over the circuits provided under this Agreement.

14. If customer is a corporation, partnership or other business entity, the individual agreeing to these terms has full authority and power to enter into this agreement. No terms or conditions in any purchase order or other document shall supersede the terms of this Agreement.

Eligibility Queries Options and Work Flows

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

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.

The provider must decide whether to:
e. 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;
f. Continue to use LU 6.2 connection where it will continue to be supported to obtain 271 data;
g. Continue to use a private network connection, where it will continue to be supported, to connect to a data center to obtain 271 data;
h. Establish a direct connection with the data center via IVANS for use of the 270/271; or
i. 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.

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

    j.   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;

    k. 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.

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

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

The contractor must:

    l.   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);

    m. 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 your own front end;

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

    o.   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.

p. 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);

q. 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.