Program Memorandum Intermediaries

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

Transmittal A-02-013 **Date: FEBRUARY 8, 2002**

CHANGE REQUEST 2009

SUBJECT: Implementation of the Health Insurance Portability and Accountability Act (HIPAA) Health Care Eligibility Benefit Inquiry/Response Transaction (270/271) Standard

This Program Memorandum (PM) provides instructions for fiscal intermediaries (FIs) and their standard systems and for the common working file (CWF) on Medicare requirements for implementation of version 4010 of the Accredited Standards Committee (ASC) X12N 270/271 Health Care Eligibility Inquiry and Response format as established in the 004010X092 Implementation Guide (IG). In order to implement the HIPAA administrative simplification provisions, the 270/271 has been named under 45 CFR 162 as the electronic data interchange (EDI) standard for Health Care Eligibility Benefit Inquiry/Response. Intermediaries are required to implement a real time version 4010 270/271 eligibility inquiry/response. All other real time formats for health care eligibility inquiry and response, other than DDE, become obsolete October 16, 2003.

I. X12 Documentation

The version 4010 implementation guide for the 270/271 standard may be found at the following web site: www.wpc-edi.com/HIPAA. The 270/271 is a "paired" transaction (the 270 is an in-bound eligibility inquiry and the 271 is an out-bound eligibility response).

II. Automated Response Unit (ARU) Requirements

If an intermediary (FI) operates an automated response unit (ARU) capability for providers to request and receive eligibility information, then the FI may continue to do so. ARUs are not considered EDI and are not affected by the HIPAA requirements. Nor do they impact response time requirements for the standard transactions implemented under HIPAA.

III. Implementation Requirements

A. On-Line Electronic Data Interchange – CWF will supply a software module that will allow FIs to implement eligibility information in an on-line immediate response environment. There are two solutions that will be included in the module; solution number 1, CWF Software Module, and solution number 2, TCP/IP Connection. FIs are required to implement solution 1. FIs may, but are not required to, implement solution 2 at this time. CMS will release future instructions for the TCP/IP connection. Both solutions are explained below.

1. **CWF Software Module** -- The CWF maintainer (CWFM) will develop and maintain the software that will support the 270/271 in real time. This software will be distributed to all FIs to be installed into the FIs systems for the implementation of the 270/271. The software will translate the 270 into the HUQA inquiry, and the HUQA response into the 271. The software will perform standard syntax edits as well as implementation guide edits, and will operate at each FI or its processing data center

The software will provide online access to a security file (to be defined by CWF) maintained by each FI containing security access data for clearinghouses, vendors, and providers to validate that each provider is eligible to view the requested data for themselves, or that each submitter is eligible to view the requested data for the provider.

The CWF module will capture audit trail data for real time (270/271) and DDE eligibility transactions. Response time must be similar to the current response time supported for LU6.2 real time eligibility inquiries. Provider access can be either direct or through the use of a vendor. The provider/vendor would be required to have supporting software and technical expertise to implement.

Details of the audit trail and security file data elements will be made available to FIs in a subsequent PM no later than March 31.

2. **TCP/IP Connection** – FIs will build upon their existing network connectivity to also provide a TCP/IP port connecting to the CWF supplied module. The CWF module will provide a TCP/IP socket interface to the same eligibility function as the LU6.2 interface. The interface also runs in a CICS mainframe environment (the same as the LU6.2 interface). Providers would dial in to the FIs gateway and connect directly to the CWF module through an IP socket. The provider/vendor would be required to have supporting software and technical expertise to implement. Additional details for this implementation will be made available to FIs in a subsequent PM.

The 271 was designed to enable reporting of standard and implementation guide 270 edits, and does not require the issuance of a 997 to report standard-level rejects, or an alternate report for notification of implementation guide-level rejects. A TA1 or a 997 must be used to reject a 270 when the data cannot be translated, or if the 270 are rejected for security access reasons. A TA1 or 997 for a 270 submitted in a real-time mode must be issued as quickly as the 271 would have been issued had the 270 been valid. CWF will generate the 997.

FIs are required to accept a 270 query and respond with a 271 in a real time immediate response mode. After October 16, 2003, FIs may not continue to operate any other format or version for real time (non-DDE) requests/responses for eligibility information.

B. CWF HIQA and Standard Systems Direct Data Entry (DDE) Eligibility Inquiry--HIPAA uses the term "direct data entry" generically to refer to a type of functionality operated by many different payers under a variety of titles. Within this instruction, the acronym DDE is being used to refer to any type of direct data entry system maintained by Medicare intermediaries, or standard system maintainers. DDE was specifically permitted to continue in the Transactions Final Rule (45 CFR162.923), with the stipulation that direct data entry is subject to "...the applicable data content and data condition requirements of the standard when conducting the transaction. The health care provider is not required to use the format requirements of the standard."

Data content conformity means that the same information permitted or required by the 271-version 4010 implementation guide must be reported in the eligibility screens (DDE outbound). The DDE outbound may not report a data element for eligibility purposes that is not included in the 271, exceeds the maximum length of the data element in the 271, does not meet the minimum length for the data element in the 271, or that does not meet the 271 requirement that the data element be numeric, alpha-numeric, or meet another characteristic as specified in the 271. The standard system cannot issue a response with information above and beyond the information in the 271. X12 standard implementation guides include data element length and characteristics in their definition of data attributes.

Conformity does not mean that a DDE screen that includes eligibility information must display each of the data qualifiers or other means of data identification contained in the 271 version 4010 implementation guide. DDE screens typically identify, explicitly or by context, the type of information being reported in a field, e.g., would identify if a number represents a health insurance claim number, date of birth, or etc. DDE screens would not be expected to use a qualifier contained in the 271 to identify data type if otherwise evident in the design or content of the DDE screen.

The standard system maintainers must map the DDE eligibility data elements to the 270/271 version 4010 implementation guide to determine if the DDE eligibility data elements meet the data content and conformity requirements above. If the standard system maintainer determines that DDE screen changes are required for data content and conformity requirements, the maintainer must modify the DDE screens to conform to the 271 version 4010 implementation guide.

If an FI currently supports the DDE functionality, then the FI must continue to do so.

CWF will be responsible for the data content and conformity requirements of HIHO, the HMO DDE eligibility process.

IV. Restricting and Controlling Access to Eligibility Information

FIs will allow Medicare certified providers, and their agents access to beneficiary eligibility data as long as an EDI Enrollment Form is on file (see MIM *Part 3 section* 3601.4) for that entity, and to network service vendors if there is an EDI Enrollment Form and EDI Network Service Agreement on file (see MIM *Part 3 section* 3601.8).

CWF will determine the appropriate information the provider is qualified to receive by the provider type; e.g., psych, HMO, home health, or other provider. The appropriate information will be displayed in a subsequent PM no later than March 31.

V. Audit Trail Requirements

The CWF module will capture the audit trail data (control information, sender/receiver information, etc.) for real time and DDE eligibility transactions. The standard systems will develop a program that will allow FIs to use the audit trail data to compare inquiry volume to paid claim volume. The FIs will generate a quarterly report using the standard systems software that will detect unusual volumes of eligibility submissions by providers. The audit trail file will contain such elements as the date/time, the HICN, the provider number, the vendor ID, etc. The appropriate information will be displayed in a subsequent PM no later than March 31.

Each quarter, the FIs will run the program developed by the standard system that compares inquiry volume to paid claim volume for use by the FIs. The standard system software will use the audit file created by CWF to tally the inquiries by provider, and then compare that total to the number of claims paid for that provider during the same quarter. Neither the standard systems nor the FIs are responsible for matching a particular inquiry with a particular claim. The sole purpose of the standard system software is to create counts and a ratio.

The claims to inquiry ratio should be at least 80 percent. This means that for every 100 inquiries submitted, we expect there to be 80 claims submitted for each provider. If the claim to inquiry ratio does not exceed 80 percent from a given provider, the FI must contact the provider to clarify inquiry volume expectations and restrictions. If there is a problem or the behavior continues, the FI must remove the provider from the FIs eligibility access system.

VI. Security Requirements

The FIs will be responsible for authenticating the User ID and Password of the submitter at the time of connection to the FI or data center for both DDE inquiry as well as real time inquiry. CWF will provide the FIs application level security module to validate that each submitter is eligible to view the requested data for the provider. The data to validate this application level authentication will reside in a CWF defined file at the FI or its data center. CWF will provide modules for the FIs to maintain and enter information in the CWF defined Security File. Details of the contents for this Security file will be made available to FIs in a subsequent PM no later than March 31. We expect this file to contain such elements as the vendor ID, associated with any providers which have been approved for that vendor, as well as the provider number of any providers that will submit queries directly.

CMS will continue to hold the FIs responsible for the privacy and security of eligibility transactions sent directly to them from providers, and require FIs to be able to associate each inquiry with a provider. However, FIs must not require providers to send userIDs and passwords within the

eligibility inquiry transactions. Provider authentication must be established outside of the transaction. CMS will hold network service vendors responsible for the privacy and security of eligibility transactions sent directly to them from providers that contract their services for eligibility transactions, and vendors must also be able to associate all inquiries with their providers. Network service vendors must not require providers to send userIDs and passwords within the eligibility transaction.

As is currently required, the FI must continue to have three items on file for each provider for which a vendor submits a 270. The required items are the Network Service Agreement, the EDI Agreement and the letter from the provider documenting their choice of a vendor.

VII. Testing

The schedule for testing is as follows:

- CWF production date – July 1, 2002;
- Standard systems production date – August 1, 2002 (this production date only relates to DDE changes and the report generation software);
- Testing with FIs – During the month of June 2002 (the FIs will not need the standard system software to test the actual 270/271 process with CWF)
- Testing with Claredi – During the month of August; contractors should be certified by August 31, 2002;
- Testing with providers/vendors – Beginning September 1, 2002 FIs should notify providers/vendors as of this date that the FI is ready for testing.

The current HUQA transaction will run parallel with the 270/271 through October 31, 2003 FIs are not required to conduct compatibility testing for each provider or vendor who elects to use the version 4010 270/271, but are required to test with each provider and vendor that requests such testing. If FIs do not have the funds to test with providers/vendors, then testing should be scheduled for FY03. FIs will notify each provider and vendor regarding testing requirements and dates.

CMS requires FIs to be certified via a third party HIPAA testing and certification system to ensure they can receive a HIPAA compliant inbound 270, and send a HIPAA compliant 271 transaction. This service will be performed by Claredi. FIs must be certified by August 30, 2002.

FIs will send '270' test cases that FIs have used in current testing environment to the Claredi website. Claredi will generate variations of the '270' test cases filling in those gaps to ensure all functionality of the transaction is tested. FIs will download the '270' test cases and use those '270' test cases to generate '271' eligibility response transactions. Claredi will perform the necessary analysis and reporting. For more details on certification, please see CR 1954, transmittal number AB-01-169, Transaction Certification and Testing.

VIII. Provider and Clearinghouse Outreach—What FIs Must Tell Providers:

- By May 1, FIs must provide information in a regularly scheduled news bulletin regarding the implementation of the ANSI X12 270/271 to their providers, third-party provider billing services, provider clearinghouses, and vendors. FIs must also inform providers, billing services, clearinghouses, and vendors that if they want to send and receive the 270/271, they must contact their FIs to establish connectivity for real-time 270/271 eligibility/benefit inquiry capability;

- EDI requests for eligibility data must be submitted via a 270 version 4010 query effective October 2003, and that each valid 270 will be issued a 271 version 4010 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 continue to support. FIs must notify all providers that receive eligibility data via DDE at least 60 days before implementation of the eligibility related changes to be made to the DDE screens;

- A provider that prefers to obtain eligibility data in an EDI format but who does not want to use a 270/271 may contract with a clearinghouse to translate the information on its behalf; however, that provider would be liable for those clearinghouse costs;

- The version 4010 270/271 implementation guide can be downloaded without charge from www.wpc-edi.com/HIPAA.

- Providers who want to test to assure system compatibility of version 4010 of the 270/271 must schedule testing with their FI;

- There is no Medicare charge for this system testing; and

- Although Medicare will furnish 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 the standards implementation guides. Providers who feel they have a need to obtain such in-depth training for their staff are expecting to obtain training of that nature from commercial vendors, their clearinghouse, or through standards development organizations.

IX. Cost Issues

Since Medicare had not previously required use of any version of the 270/271, contractors are entitled to reasonable costs for implementation, testing, and transition to the 270/271 version 4010. These costs should have been included in the SBRs that were due on November 26, 2001.

HIPAA established requirements binding on all health care payers, not only on Medicare. HIPAA did not provide for Federal funding of implementation of the Administrative Simplification provisions by health care payers. As with other system and program changes that impact a Medicare contractor's parent company's private/commercial lines of business, as well as its Medicare processing activities, direct and indirect costs related to such changes must be proportionately shared by the impacted lines of business, and not charged to Medicare in total. Programming, transition, and operational costs related to a corporate clearinghouse operated by a Medicare contractor's parent company, or any other profit or non-profit line of business of the parent company required to support Medicare processing under the terms of its Medicare contract, may not be charged in total or in part to the Medicare program.

The effective date for this PM is July 1, 2002.

The implementation date for CWF is July 1, 2002.

The implementation date for standard systems is August 1, 2002.

See section IX, Cost Issues, for implementation cost information.

This PM may be discarded after October 31, 2004.

Medicare contractor questions concerning this PM may be directed to Jean Gross, (410) 786-6159, or e-mail JGROSS3@CMS.HHS.GOV.

Any provider, clearinghouse or other vendor questions related to this PM should be directed to their servicing Medicare intermediary.