Medicare Claims Processing Manual
Chapter 31 - ANSI X12N Formats Other than Claims or Remittance

Table of Contents
(Rev. 1149, 01-05-07)

10 - X12N Health Care Eligibility Benefit Inquiry and Response 270/271 Implementation

(Rev. 583, Issued: 06-15-05, Effective: 05-20-05, Implementation: 08-22-05)

PM AB-03-036

10.1 - Background

(Rev. 583, Issued: 06-15-05, Effective: 05-20-05, Implementation: 08-22-05)

This section provides information on Medicare's implementation of the ANSI ASC X12N 270/271, version 4010A1 implementation guide which was adopted as the national standard for the health care eligibility benefit inquiry and response under the Health Insurance Portability and Accountability Act (HIPAA). Current carriers, intermediaries and their data centers will not be responding to or processing 270 transactions for Medicare beneficiaries.

10.2 - Eligibility Extranet Workflow

(Rev. 892, Issued: 03-24-06, Effective: 06-26-06, Implementation: 06-26-06)

The Centers for Medicare and Medicaid Services (CMS) is making changes to its Information Technology infrastructure to address standards for Medicare beneficiary eligibility inquiries. This approach will create the necessary database and infrastructure to provide a centralized HIPAA compliant 270/271 health care eligibility inquiry and response in real-time.

The CMS is using a phased approach for providing this eligibility transaction on a real-time basis:

1. Extranet: In June of 2005, Clearinghouses, certain providers and trading partners (as described below) will be permitted to submit 270s via the CMS AT&T communication Extranet (the Medicare Data Communication Network or MDCN). This Extranet is a secure closed private network currently used to transmit data between Medicare Fee-for-Service (FFS) contractors and CMS.

2. Internet: We expect to provide limited Internet access to the 270/271 transaction later this year. Instructions on accessing eligibility data via this method will be provided prior to the time Internet access becomes available.

All electronic 270 files will be processed at the CMS data center. The CMS data center will use a single consolidated national eligibility database to respond to the eligibility inquiries.

Access Process for Clearinghouses/Provider

September 1, 2005 all submitters who have been authenticated by CMS to conduct 270/271 transactions with CMS will be required to complete a TRADING PARTNER AGREEMENT FOR SUBMISSION OF 270s TO MEDICARE ON A REAL-TIME BASIS. This agreement outlines security and privacy procedures for the submitters requesting access to the Medicare beneficiary database. The Medicare Eligibility Integration Contractor (MEIC) will transmit via e-mail the TRADING PARTNER AGREEMENT FOR SUBMISSION OF 270s TO MEDICARE ON A REAL-TIME BASIS to each authenticated submitter. Each submitter should complete the form in its entirety and transmit it back via e-mail to MCAREHD@emdeon.com.

Starting October 1, 2005 in order to obtain access to the CMS 270/271 Medicare Eligibility transaction via the MDCN a Submitter will access the appropriate forms at www.cms.hhs.gov/AccessToDataApplication. The first form to be completed is the TRADING PARTNER AGREEMENT FOR SUBMISSION OF 270s TO MEDICARE ON A REAL-TIME BASIS. This agreement outlines security and privacy procedures for the submitters requesting access to the Medicare beneficiary database. The submitter must electronically provide the information requested on the form and click on the appropriate assurances. If Submitter does not consent to the terms of the agreement, by appropriately completing the form the access process will be terminated.

If Submitter checks the appropriate boxes of the agreement and supplies the information requested, a copy of the completed form will be electronically submitted to the CMS 270/271 Medicare Eligibility Integration Contractor (MEIC) for security authentication. The access process will then continue, and the Submitter will be directed to complete an MDCN connectivity form and submit it electronically in order to be connected to the 270/271 eligibility database.

CMS staff will ensure that all of the necessary information is provided on the form, as well as ensure the complete connectivity to the 270/271 application. The MEIC will be responsible for contacting the Clearinghouses, providers, and trading partners to authenticate the accessing entity's identity. Once authentication has been completed, the MEIC will provide the Clearinghouses, Providers, and Trading Partners with a submitter ID that is required to be used on all 270/271 transactions. Testing will be coordinated by the MEIC. After successful testing, 270 production inquiries may be sent real-time. Please note that in order to access the MDCN, an entity must on its own obtain the necessary telecommunication software from the AT&T reseller.

The current AT&T resellers and contact numbers are listed below:

IVANS: www.ivans.com

1-800-548-2675

McKesson: www.mckesson.com

1-800-782-7426, option 5, then key option 8

Helpdesk Support

The MEIC will provide help desk support during the hours of 7:00am - 9:00pm eastern time Monday through Friday. The phone number is: 1-866-324-7315. The email address for the helpdesk is: MCARE@cms.hhs.gov.

Telecommunications Wrapper

Communications through the extranet to the CMS data center will be via the TCP/IP streaming socket protocol. Trading Partners can submit multiple 270 transactions; it will not be necessary to wait for a response before triggering the next 270. Trading partners must ensure that the session remains connected until all responses are received. Each submitted transmission shall contain one 270 transaction with only one ISA and IEA segment, along with a transmission wrapper around the 270 transaction. There will be no handshake after the connection is accepted with the first submitted transmission.

Outbound response transactions will have the same format transmission wrapper. The response to the submitter will be returned in the same session in which the 270 was submitted.

Standard format of the TCP/IP Transaction Wrapper:

SOHLLLLLLLLLLSTX<HIPAA 270 Transaction>ETX

SOH = Required (1 position), must be EBCDIC or ASCII - 01

LLLLLLLLLL = Required (10 positions), Right justified with zero padded

Note: Length of the HIPAA 270 transaction not including Transmission wrapper data.

STX = Required (1 position), must be EBCDIC or ASCII - 02

<HIPAA 270 Transaction> = Required (HIPAA 270 - ISA - IEA),

ETX = Required (1 position), Must be EBCDIC or ASCII -03

NOTE: For more detail about SOH, STX and ETX, see the Health Care Eligibility Benefit Inquiry and Response 270/271 ASC X12 Extended Control Set.

270 Inquiry Requirements

The ISA08 (interchange receiver id) and the GS03 (application receiver's code) on the 270 transactions must contain "CMS", left justified space filled.

CMS will return certain data elements on the 271 response only when certain service type codes are sent on the 270. Other core data elements will be included in each 271 response, regardless of service type codes, when applicable. Both the core and the additional data elements are listed below.

CMS will utilize the search option as listed in the 270/271 implementation guide (section 1.3.8) requiring the patient's member id (HIC number), patient's full first name, patient's full last name, and patient's date of birth.

Proprietary Error Messages

Proprietary error messages will be sent only when the ISA segment of the 270 transaction cannot be read making it impossible to formulate an ISA segment for the response. The format of the proprietary message is described below:

Description	Content	Size	Comments
Transaction	Transaction ID	04 characters	"HETS"
Transaction Reference Number	Reference #	30 characters	Reference Number for tracking
Date Stamp	System Date	08 Characters	CCYYMMDD
Time Stamp	System time	09 Characters	HHMMSSSSS
Response Code	Error Code	02 Characters	See Below
	ISA Response code	" I"	Incoming ISA cannot be read
	Delimiter Response code	" D"	Delimiter could not be identified
Message Code	Error Code	08 Characters	Error code
Message Text Description	Error Descriptions	70 Characters	Description of error

271 Response Data Elements

If a service type code is submitted in a 270 that does not trigger additional Medicare data elements, the following data elements will be returned in the 271 as applicable:

271 INFORMATION RETURNED	LOOP	SEGMENT	ELEMENT	DATA VALUE
Part A/B	2110C	EB	EB01	1
Entitlement/Term Dates			EB02	IND
			EB04	MB or MA

	2110C	DTP	DTP01 DTP02 DTP03	307 RD8 or D8 Date(s)
Beneficiary Address	2100C	N3 N4	N301 N302 N401 N402 N403	Address Address City State Code Zip Code
Deductible - Part B	2110C	EB	EB01 EB03 EB04 EB06 EB07	C 96 MB 29 Amount
	2110C	DTP	DTP01 DTP02 DTP03	292 RD8 Applicable Calendar Year
MCO Data	2110C	EB	EB01 EB03 EB04	R 30 HN

	2110C	REF	REF01 REF02	18 MCO ID
	2110C	DTP	DTP01 DTP02 DTP03	290 RD8 or D8 Date(s)
	2120C	NM1	NM101 NM102 NM103	PRP 2 Insurer Name
	2120C	N3	N301 N302	Address Address
	2120C	N4	N401 N402 N403	City State Code ZIP Code
MSP Data	2110C	EB	EB01 EB02 EB03 EB04	R Ind 30 12, 13, 14, 15, 16, 41, 42, 43, 47
	2110C	REF	REF01 REF02	IG Policy Number
	2110C	DTP	DTP01 DTP02 DTP03	290 RD8 or D8 Date(s)

	2120C	NM1	NM01	PRP
			NM102	2
			NM103	Name
	2120C	N3	N301	Address
			N302	Address
	2120C	N4	N401	City
			N402	State Code
			N403	Zip Code
Home Health Data	2110C	EB	EB01	X
			EB03	42
			EB04	MA
			EB06	26
	2110C	DTP	DTP01	193 or 194
			DTP02	D8
			DTP03	Date(s)
	2110C	MSG	MSG01	HHEH Start Date
				HHEH End Date
				HHEH DOEBA
				HHEH DOLBA
Hospice Data	2110C	EB	EB01	X
			EB03	45
			EB04	MA
			EB06	26

		DTP	DTP01 DTP02 DTP03	292 D8 or RD8 Dates

If one or more of the following service type codes are submitted in a 270, the following additional data elements will be returned in the 271, as applicable.

Service Type Code	LOOP	SEGMENT	ELEMENT	DATA VALUE
14	2110C	EB	EB01 EB03 EB04	D 14 MB
	2110C	DTP	DTP01 DTP02 DTP03	356 D8 Date
	2110C	DTP	DTP01 DTP02 DTP03	198 D8 Date
	2120C	MSG	MSG01	Transplant Discharge Date
15	2110C	EB	EB01 EB03 EB04	D 15 MA
	2110C	DTP	DTP01 DTP02 DTP03	356 D8 Date

	2110C	DTP	DTP01	198
			DTP02	D8
			DTP03	Date
	2120C	MSG	MSG01	Transplant Discharge Date
42	2110C	EB	EB01	X
			EB03	42
			EB04	MA
	2120C	NM1	NM101	PR
			NM102	2
			NM103	Name of RHHI
			NM108	PI
			NM109	00011, 00180, 00380, 00450, 00454
	2120C	PRV	PRV01	HH
			PRV02	9K
			PRV03	Provider number

47	2110C	EB	EB01	C
		Part A Deductible	EB03	47
			EB04	MA
			EB06	29
			EB07	Amount
		DTP		
		Hospital Admission	DTP01	435
			DTP02	RD8
			DTP03	Dates
	2110C	EB	EB01	F
		Hospital Days Remaining	EB03	47
			EB04	MA
			EB06	29
			EB09	DY
			EB10	Days
		DTP		
		Hospital Admission	DTP01	435
			DTP02	RD8
			DTP03	Dates

	2110C	EB	EB01	A
		Co-Insurance Days Remaining	EB03	47
			EB04	MA
			EB06	29
			EB07	Amount Per Day
			EB09	DY
			EB10	Days
		DTP		
		Hospital Admission	DTP01	435
			DTP02	RD8
			DTP03	Dates
	2110C	EB	EB01	K
		Lifetime Reserve Days	EB03	47
			EB04	MA
			EB06	33
			EB09	LA
			EB10	Days

AG	2110C	EB	EB01	F
		Hospital Days Remaining	EB03	47
			EB04	MA
			EB06	29
			EB09	DY
			EB10	Days
		DTP		
		Hospital Admission	DTP01	435
			DTP02	RD8
			DTP03	Dates
	2110C	EB	EB01	A
		Co-Insurance Days Remaining	EB03	47
			EB04	MA
			EB06	29
			EB07	Amount Per Day
			EB09	DY
			EB10	Days
		DTP		
		Hospital Admission	DTP01	435
			DTP02	RD8
			DTP03	Dates

	2110C	EB	EB01	K
		Lifetime Reserve Days	EB03	47
			EB04	MA
			EB06	33
			EB09	LA
			EB10	Days
	2110C	EB	EB01	F
		SNF Days Remaining	EB03	AG
			EB04	MA
			EB06	29
			EB09	DY
			EB10	Days
		DTP		
		SNF Admission	DTP01	435
			DTP02	RD8
			DTP03	Dates

	2110C	EB	EB01	A
		Co-Insurance SNF Days Remaining	EB03	AG
			EB04	MA
			EB06	29
			EB07	Amount Per Day
			EB09	DY
			EB10	Days remaining
		DTP SNF Admission	DTP01	435
			DTP02	RD8
			DTP03	Dates

10.3 – *Medicare HIPAA Eligibility Transaction System Inquiries Rules of Behavior*

(Rev. 1149, Issued: 01-05-07, Effective: 01-01-07, Implementation: 04-02-07)

The Centers for Medicare & Medicaid Services (CMS) is committed to maintaining the integrity and security of health care data in accordance with applicable laws and regulations. Disclosure of Medicare beneficiary eligibility data is restricted under the provisions of the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996 (HIPAA.) The provider Medicare beneficiary eligibility transaction is to be used for conducting Medicare business only.

In October 2005, the CMS began offering to Medicare providers and clearinghouses, the HIPAA 270/271 beneficiary eligibility transaction in a real-time environment via the *CMS AT&T communication Extranet. In June 2006, CMS began to pilot an Internet application for eligibility information. Over time this application will be available to an increasing number of Medicare providers.*

This document reiterates your responsibility in obtaining, disseminating, and using beneficiary's Medicare eligibility data. It further explains the expectations for using the *HIPAA 270/271 Extranet application and the Eligibility Internet application. Acceptance of these Medicare* Rules of Behavior is necessary *in order to gain access to the system. Violating these rules of behavior and/or* other CMS data privacy and security rules could result in revoked access and other penalties.

CMS monitors beneficiary eligibility inquiries. Submitters identified as having aberrant behavior (e.g., high inquiry error rate or high ratio of eligibility inquires to claims submitted) may be contacted to verify and/or address improper use of the system or, when appropriate, be referred for investigation.

Authorized Purposes for Requesting Medicare Beneficiary Eligibility Information

In conjunction with the intent to provide health care services to a Medicare beneficiary, authorized purposes include to:

- *Verify eligibility, after screening the patient to determine Medicare eligibility, for Part A or Part B of Medicare*
- *Determine beneficiary payment responsibility with regard to deductible/co-insurance*
- *Determine eligibility for services such as preventive services*
- *Determine if Medicare is the primary or secondary payer*
- *Determine if the beneficiary is in the original Medicare plan, Part C plan (Medicare Advantage) or Part D plan.*
- *Determine proper billing*

Unauthorized Purposes for Requesting Beneficiary Medicare Eligibility Information

The following are examples of unauthorized purposes for requesting Medicare beneficiary eligibility information:

- *To* determine eligibility for *Medicare without screening the patient to determine if they are Medicare eligible*
- To acquire the beneficiary's health insurance claim number

Medicare eligibility data is only to be used for the business of Medicare; such as preparing an accurate Medicare claim or determining eligibility for specific services. *Providers authorized staff are expected to use and disclose protected health information according to the CMS regulations. The HIPAA Privacy Rule mandates the protection and privacy of all health information. This rule specifically defines the authorized uses and disclosures of "individually-identifiable" health information. The privacy regulations ensures privacy protections for patients by limiting the ways that physicians, qualified non-physician practitioners, suppliers, hospitals and other provider covered entities can use a patients' personal medical information.*

Criminal Penalties

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HHS may impose civil money penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement. That penalty may not exceed $25,000 per year for multiple violations of the identical Privacy Rule requirement in a calendar year. A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces a fine of $50,000 and up to one-year imprisonment. The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses, and to $250,000 and up to ten years imprisonment if the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. Criminal sanctions will be enforced by the Department of Justice.

Trading Partner Agreement Violation

42 U.S.C. 1320d-6 authorizes criminal penalties against a person who, "knowingly and in violation of this part ... (2) obtains individually identifiable health information relating to an individual; or (3) discloses individually identifiable health information to another person." Offenders shall "(1) be fined not more than $50,000, imprisoned not more than 1 year, or both; (2) if the offense is committed under false pretenses, be fined not more than $100,000, imprisoned not more than 5 years, or both; and (3) if the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, be fined not more than $250,000, imprisoned not more than 10 years, or both."

False Claim Act

Under the False Claims Act, 31 U.S.C. §§ 3729-3733, those who knowingly submit, or cause another person or entity to submit, false claims for payment of government funds are liable for three times the government's damages plus civil penalties of $5,500 to $11,000 per false claim.

Accessing Beneficiary Eligibility Data: Provider Responsibilities

As a provider or an individual employed by the provider, you will be responsible for the following:

- Before you request Medicare beneficiary eligibility information and at all times thereafter, you will ensure sufficient security measures to associate a particular transaction with the particular employee.

- You will cooperate with CMS or its agents in the event that CMS has a security concern with respect to any eligibility inquiry.

- You will promptly inform CMS or one of CMS's contractors in the event you identify misuse of "individually-identifiable" health information accessed from the CMS database.

- Each eligibility inquiry will be limited to requests for Medicare beneficiary eligibility data with respect to a patient currently being treated or served by you, or who has contacted you about treatment or service, or for whom you have received a referral from a health care provider that has treated or served that patient.

Clearinghouse Use of the HIPAA 270/271 Extranet Transaction

The Medicare Electronic Data Interchange (EDI) Enrollment process provides for the collection of the information needed to successfully exchange EDI transactions between Medicare and EDI trading partners and establishes the expectations for both parties for the exchange.

As a reminder, along with other EDI provisions, you agreed to use sufficient security procedures (including compliance with all provisions of the HIPAA security regulations) to ensure that all transmissions of data are authorized and protect all beneficiary-specific data from improper access. The clearinghouse is responsible for the privacy and security of eligibility transactions with providers.

The CMS instructions allow release of eligibility data to providers or their authorized billing agents for the purpose of preparing an accurate Medicare claim or determining eligibility for specific ser*vices.* Such information may not be disclosed to anyone other than the Medicare provider *and/or* supplier*, seeking to file a* claim.

Access will be prohibited or suspended if there is a record of prior violation of a clearinghouse agreement that would indicate that beneficiary data could be at risk of improper disclosure if access was approved for the clearinghouse.

Per the EDI agreement, to receive access to eligibility data on behalf of providers, you must adhere to the following rules:

- Each provider that contracts with a clearinghouse must sign a valid EDI Enrollment Form *and be approved by a Medicare contractor* before eligibility data can be sent to the third party;

- *Each clearinghouse must sign appropriate agreement(s) (i.e. Rules of Behavior, Trading Partner Agreement and Attestation Form) directly with CMS and/or one of CMS's contractors;*

- The clearinghouse must be able to associate each inquiry with the provider *or billing service* making the inquiry. That is, for each inquiry made by a clearinghouse, that vendor must be able to identify the provider making the

request for each beneficiary's information and be able to assure that eligibility responses are routed only to the submitter that originated each request.

CMS requires that trading partners who wish to conduct transactions with CMS provide certain assurances as a condition of receiving access to the Medicare database for the purpose of conducting real-time transactions.

- You must not submit an eligibility inquiry except as an authorized agent of the health care provider and pursuant to a business associate contract, as required by 45 C.F.R. §§164.314(a) and 164.504(e), with the health care provider.

- If you submit a 270 that has been prepared by a provider/supplier utilizing your services, you are responsible for ensuring that the provider/supplier provides sufficient security measures, including user ID and password, to be able to associate the 270 *with an individual submitting the transaction.*

Provider/Supplier *Use of the HIPAA 270/271 Extranet Transaction*

The EDI Enrollment process must be executed by each provider that submits/receives EDI either directly to or from Medicare or through a third party (a billing agent or clearinghouse*)* *in* order to exchange EDI transactions with Medicare.

As a reminder, along with other EDI provisions*, in signing the EDI enrollment form*, you agreed to use sufficient security procedures (including compliance with all provisions of the HIPAA security regulations) to ensure that all transmissions of documents are authorized *and that you will* protect all beneficiary-specific data from improper access.

The CMS instructions allow release of eligibility data to providers or their authorized billing agents for the purpose of preparing an accurate Medicare claim or determining eligibility for specific services. You are responsible for ensuring sufficient security measures, including user ID and password, to be able to associate the 270 with an individual submitting the transaction.

Provider Use of Eligibility Internet Application

As a user of the eligibility Internet application, you are required to register in IACS (Individual Authorized Access to CMS Computer Services) in order to gain access to the eligibility application. The IACS system is an on-line application used to register and provision authorized users for access to CMS applications and systems. You will be required to provide the following information:

- *User social security number*

- *Email address*

This information is needed by the system to identify you and to allow the system to communicate with you through email.

You will also be required to adhere to the security requirements for users of CMS computer systems and to the basic desktop security measures to ensure the security of Medicare beneficiary personal health information. You must not:

- *Disclose or lend your identification number and/or password to someone else. They are for your use only and serve as your electronic signature. This means that you may be held responsible for the consequences of unauthorized or illegal transactions.*
- *Browse or use CMS data files for unauthorized or illegal purposes.*
- *Use CMS data files for private gain or to misrepresent yourself or CMS.*
- *Make any disclosure of CMS data that is not specifically authorized.*

Again, violation of these security requirements could result in termination of systems access privileges and /or disciplinary/adverse action up to and including legal prosecution. Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or operated computer system.

The CMS instructions allow release of eligibility data to providers or their authorized billing agents for the purpose of preparing an accurate Medicare claim or determining eligibility for specific services.

Extranet and Internet Beneficiary Data Matching Requirements

Prior to the release of a 271 beneficiary-specific eligibility response information, 270 inquires must have correct information including: the beneficiary first and last name which must match the name on the Medicare card, the assigned Medicare Claim Number (also referred to as the Health Insurance Claim Number (HICN)), including both alpha and numerical characters, and the beneficiary date of birth.

Note to Providers: The Medicare beneficiary should be the first source of health insurance eligibility information. When scheduling a medical appointment for a Medicare beneficiary, remind them to bring, on the day of their appointment, all health insurance cards showing their health insurance coverage. This will not only help you determine who to bill for services rendered, but also give you the proper spelling of the beneficiary's first and last name and identify their Medicare Claim Number as reflected on the Medicare Health Insurance card. If the beneficiary has Medicare coverage but does not have a Medicare Health Insurance card, encourage them to contact the Social Security Administration at 1-800-772-1213 to obtain a replacement Medicare Health Insurance card. Those beneficiaries receiving benefits from the Railroad Retirement Board (RRB)

can call 1-800-808-0772 to request a replacement Medicare Health Insurance card from RRB.

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

(Rev. 1, 10-01-03)

AB - 01-106

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

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

20.1 - Transmission Requirements

(Rev. 1, 10-01-03)

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

20.1.1 - Batch Transactions

(Rev. 1, 10-01-03)

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

20.1.2 - Online Direct Data Entry (DDE)

(Rev. 1, 10-01-03)

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

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

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

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

Shared system maintainers must map the DDE claim status data elements to the 276/277 implementation guide to determine if the DDE claim status data elements meet the

conformity requirements above. If needed, changes must be made to enable contractor DDE claim status data elements to conform.

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

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

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

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

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

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

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

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

20.1.3 - Interactive/Online (Non-DDE)

(Rev. 1, 10-01-03)

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

- Terminate that support effective October 2003; or

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

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

(Rev. 1, 10-01-03)

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

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

made available as quickly as the 277 response would have been (had it been error free) whether the response is the TA1, 997 or the shared system generated error report.

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

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

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

C. The shared system either:

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

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

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

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

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

20.3 - Flat Files

(Rev. 1, 10-01-03)

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

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

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

20.4 - Translation Requirements

(Rev. 1, 10-01-03)

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

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

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

A contractor’s overall translation process must also:

- Convert lower case to upper case;

- Pass all spaces (default values) to the 276 flat file for fields that are not present on the inbound ANSI X12N 276. Do not generate a record on the 276 flat file if the corresponding segment is not present on the inbound ANSI X12N 276;

- Map "Not Used" data elements based upon that segment's definition, i.e., if a data element is never used, do not map it. However, if a data element is "required" or "situational" in some segments but not used in others, then it must be mapped;

- Remove the hyphen from all range of dates with a qualifier of "RD8" when mapping to the ANSI X12N-based flat file; and

- Accept multiple interchange envelopes within a single transmission.

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

The error code values are:

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

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

"b" blank will represent no error.

For example, a dollar amount with the implementation guide maximum of 18-digits would look like 12345678.90. The translator must map this amount to the X12-based flat file using the COBOL picture of S9(7)V99. The flat file amount will be 23456789{bbbbbbbbX. The "{" is the converted sign value for positive "0." The error switch value is "X" since this value exceeded the COBOL picture of S9(7)V99.

Conversion Table

1 = A	-1 = J
2 = B	-2 = K
3 = C	-3 = L
4 = D	-4 = M

5 = E	-5 = N
6 = F	-6 = O
7 = G	-7 = P
8 = H	-8 = Q
9 = I	-9 = R
0 = {	-0 = }

20.5 - Transmission Mode

(Rev. 1, 10-01-03)

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

20.6 - Restriction and Controlling Access to Claims Status Information

(Rev. 1, 10-01-03)

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

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

(Rev. 583, Issued: 06-15-05, Effective: 05-20-05, Implementation: 08-22-05)

Under the Health Insurance Portability and Accountability Act (HIPAA), all payers must use health care claim status category codes and health care claim status codes approved by the Health Care Code Maintenance Committee as applicable. At each X12 trimester meeting (generally held the months of February, June and October), the Committee may update the claim status category codes and the claim status codes. When instructed, Medicare contractors must update their claims systems to assure that the current version of these codes is used in their claim status responses. The codes sets are available at http://www.wpc-edi.com/codes/Codes.asp. Included in the code lists are specific details, including the date when a code was added, changed or deleted.

CMS will issue recurring, one-time change requests regarding the need for and deadline for future updates to these codes. Contractor and shared system changes will be made as necessary as part of a routine release to reflect applicable changes such as retirement of previously used codes or newly created codes that may impact Medicare. Shortly after the release of each code update, a provider education article will be available at http://www.cms.hhs.gov/medlearn/matters for contractors to use to conduct provider outreach.

Transmittals Issued for this Chapter

Rev #	Issue Date	Subject	Impl Date	CR#
R1149CP	01/05/2007	Revision of Chapter 31 Eligibility Rules of Behavior	04/02/2007	5431
R991CP	06/23/2006	Eligibility Rules of Behavior	07/24/2006	5138
R892CP	03/24/2006	Eligibility Transaction URL Update	06/26/2006	4366
R793CP	12/29/2005	Revision to Chapter 31-Addition of Hospice Data HIPAA270/271 Eligibility	01/23/2006	4193
R791CP	12/23/2005	Revision to Chapter 31-Addition of Hospice Data HIPAA270/271 Eligibility	01/23/2006	4193
R583CP	06/15/2005	Access Process for HIPAA 270/271 (Extranet Only)	08/22/2005	3883
R565CP	05/20/2005	Access Process for HIPAA 270/271 (Extranet Only)	08/22/2005	3883
R490CP	03/04/2005	Claims Status Code/Claim Status Category Code Update	07/05/2005	3715
R406CP	12/17/2004	Update to Health Care Claims Status Category Codes and Health Care Claim Status Codes for Use with the Health Care Claim Status Request and Response ASC X12N 276/277.	04/04/2005	3566
R230CP	07/23/2004	Update to Health Care Claims Status Category Codes and Health Care Claim Status Codes for Use with the Health Care Claim Status Request and Response (ASC X12N 276/277)	01/03/2005	3361
R096CP	02/06/2004	Health Care Claims Status Category Codes and Health Care Claim Status Codes for Use with the Health Care Claim Status Request and Response (ASC X12N 276/277)	N/A	3017
R001CP	10/01/2003	Initial Publication of Manual	NA	NA