CMS Manual System

Pub 100-04 Medicare Claims Processing

Transmittal 991

Department of Health & Human Services (DHHS)

Center for Medicare & Medicaid Services (CMS)

Date: JUNE 23, 2006

Change Request 5138

SUBJECT: Eligibility Rules of Behavior

I. SUMMARY OF CHANGES: Adding Rules of Behavior for Eligibility Access

NEW/REVISED MATERIAL
EFFECTIVE DATE: July 24, 2006
IMPLEMENTATION DATE: July 24, 2006

Disclaimer for manual changes only: The revision date and transmittal number apply only to red italicized material. Any other material was previously published and remains unchanged. However, if this revision contains a table of contents, you will receive the new/revised information only, and not the entire table of contents.

II. CHANGES IN MANUAL INSTRUCTIONS: (N/A if manual is not updated)
R = REVISED, N = NEW, D = DELETED – *Only One Per Row.*

R/N/D	Chapter / Section / SubSection / Title
N	31/10/10.3/Eligibility Rules of Behavior

III. FUNDING:
No additional funding will be provided by CMS; Contractor activities are to be carried out within their FY 2006 operating budgets.

IV. ATTACHMENTS:

One-Time Notification

**Unless otherwise specified, the effective date is the date of service.*

Attachment – Business Requirements

Pub. 100-04	Transmittal: 991	Date: June 23, 2006	Change Request 5138

SUBJECT: Eligibility Rules of Behavior

I. GENERAL INFORMATION

A. Background: This addition reiterates the responsibilities of users in obtaining, disseminating, and using beneficiary's Medicare eligibility data. It also further explains the expectations for Clearinghouses and providers using this application.

B. Policy: 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

II. BUSINESS REQUIREMENTS

"Shall" denotes a mandatory requirement
"Should" denotes an optional requirement

Requirement Number	Requirements	Responsibility ("X" indicates the columns that apply)								
		FI	RHHI	Carrier	DMERC	Shared System Maintainers				Other
						FISS	MCS	VMS	CWF	
5138.1	Contractors shall insure that the Rules of Behavior are followed.	X	X	X	X	X	X	X	X	X

III. PROVIDER EDUCATION

Requirement Number	Requirements	Responsibility ("X" indicates the columns that apply)								
		FI	RHHI	Carrier	DMERC	Shared System Maintainers				Other
						FISS	MCS	VMS	CWF	
	A provider education article related to this instruction will be available at www.cms.hhs.gov/MLNMattersArticles shortly after the CR is released. You will receive notification of the article release via the established "MLN Matters" listserv. Contractors shall post this article, or a direct link to this article, on their Web site and include information about it in a listserv message within 1 week of the availability of the provider education article. In addition, the provider education article shall be included in your next regularly scheduled bulletin and incorporated into any educational events on this topic. Contractors are free to supplement MLN Matters articles with localized information that would benefit their provider community in billing and administering the Medicare program correctly.	X	X	X						

IV. SUPPORTING INFORMATION AND POSSIBLE DESIGN CONSIDERATIONS

A. Other Instructions: N/A

X-Ref Requirement #	Instructions

B. Design Considerations: N/A

X-Ref Requirement #	Recommendation for Medicare System Requirements

C. Interfaces: N/A

D. Contractor Financial Reporting /Workload Impact: N/A

E. Dependencies: N/A

F. Testing Considerations: N/A

V. SCHEDULE, CONTACTS, AND FUNDING

Effective Date*: July 24, 2006 **Implementation Date:** July 24, 2006 **Pre-Implementation Contact(s):** Bob Huffman Robert.huffman@cms.hhs.gov (410)786-6317 **Post-Implementation Contact(s):** Bob Huffman Robert.huffman@cms.hhs.gov (410)786-6317	**No additional funding will be provided by CMS; contractor activities are to be carried out within their FY 2006 operating budgets.**

***Unless otherwise specified, the effective date is the date of service.**

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

Table of Contents
(Rev. 991, 06-23-06)

10.3 – Eligibility Rules of Behavior

(Rev. 991, Issued: 06-23-06; Effective/Implementation Dates: 07-24-06)

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.)

In October 2005, the CMS began offering to specific Clearinghouses and providers, the HIPAA 270/271 beneficiary eligibility transaction in a real-time environment via the CMS AT&T communication Extranet.

This document reiterates your responsibility in obtaining, disseminating, and using beneficiary's Medicare eligibility data. It also further explains the expectations for Clearinghouses and providers using this application. Violating these Medicare Health Benefit Eligibility Inquiry Rules of Behavior and other CMS data privacy and security rules could result in revoked access and other penalties.

Clearinghouses

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. You must be able to associate each inquiry with a provider.

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. Such information may not be disclosed to anyone other than the provider, supplier, or beneficiary for whom a claim is filed.

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

- *Each clearinghouse must sign an agreement (e.g. Network Service Vendor Agreement, Trading Partner Agreement, Attestation Form) directly with CMS or one of CMS's contractors;*
- *Each provider that contracts with a clearinghouse must sign a valid EDI Enrollment Form before eligibility data can be sent to the third party;*
- *The provider must explain the type of EDI services to be furnished by its clearinghouse in a signed statement authorizing the vendor's access to eligibility data;*

- *The clearinghouse must be able to associate each inquiry with the provider making the inquiry. That is, for each inquiry made by a provider through 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 provider that originated each request; and*
- *No access will be allowed 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.*

The access of Medicare beneficiary eligibility data is to be used for the business of Medicare only. You, and the providers you serve, when accessing Medicare eligibility data must be fully aware of this requirement and all penalties related to the misuse of "individually-identifiable" health information accessed from the CMS database. Accordingly, 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 submitted 270 to the specific person/submitter from the provider/supplier.*

Providers/Suppliers

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. Each provider that will use EDI either directly or through a billing agent or clearinghouse to exchange EDI transactions with Medicare must sign the EDI Enrollment Form and submit it to the

Carrier, DMERC, or FI with whom EDI transactions will be exchanged before any transaction is conducted.

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 documents are authorized and protect all beneficiary-specific data from improper access.

Acting on behalf of the beneficiary, providers/users of Medicare data 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.

Authentication for HIPAA 270/271 Eligibility Data

Authenticating elements that must be granted by the inquirer prior to the release of any beneficiary-specific eligibility information include:

Beneficiary last name (must match the name on the Medicare card)

Beneficiary first name or first initial (must match the information on the Medicare card)

Assigned Medicare Claim Number (also referred to as the Health Insurance Claim Number (HICN)), including both alpha and numerical characters

Date of birth

*Note**:** The Medicare beneficiary should be your 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 determining 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, encouraged 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.*

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 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 or a Part C plan (Medicare Advantage)*
- *Determine proper billing*

Unauthorized Purposes for Requesting Beneficiary Medicare Eligibility Information

- *To determine eligibility for Medicare*
- *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.

In order to obtain access to eligibility data, as a 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.*

Medicare health benefit beneficiary eligibility inquiries are monitored. Providers 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 proper use of system, made aware of educational opportunities, or when appropriate referred for investigation of possible fraud and abuse or violation of HIPAA privacy law.

Criminal Penalties

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.

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.