



## Attention all Medicare Physicians, Providers, and Suppliers!

Sign up now for the listserv appropriate for you at [https://list.nih.gov/cgi-bin/wa.exe?A0=mln\\_education\\_products-l](https://list.nih.gov/cgi-bin/wa.exe?A0=mln_education_products-l).

Get your Medicare news as it happens!

MLN Matters Number: MM5138

Related Change Request (CR) #: 5138

Related CR Release Date: June 23, 2006

Effective Date: July 24, 2006

Related CR Transmittal #: R991CP

Implementation Date: July 24, 2006

**Note:** This article was updated on November 8, 2012, to reflect current Web addresses. All other information remains unchanged.

## Rules Governing Provider/Clearinghouse Protection of Medicare Beneficiary Eligibility Information

### Provider Types Affected

Physicians, providers, suppliers, and clearinghouses who bill Medicare fiscal intermediaries (FIs), carriers, regional home health intermediaries (RHHIs), and durable medical equipment regional carriers (DMERCs), and who use the HIPAA 270/271 beneficiary eligibility transaction data in a real-time environment via the Centers for Medicare & Medicaid Services (CMS) AT&T communication Extranet

### Background

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.)

This article is a reminder to physicians/providers/suppliers of the importance of protecting Medicare beneficiary information and to use it only for authorized purposes. Be sure all your representatives and employees who have authorized access to this information are aware of the importance of protecting that information as well.

#### Disclaimer

This article was prepared as a service to the public and is not intended to grant rights or impose obligations. This article may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.

## Key Points of CR5138

---

Change Request (CR) 5138 reiterates the responsibilities of users in obtaining, disseminating, and using beneficiary's Medicare eligibility data. The following key points outline those responsibilities:

### ***EDI Enrollment***

The Medicare electronic data interchange (EDI) enrollment process must be executed by each physician/provider/supplier that submits/receives EDI either directly to or from Medicare or through a third party, such as a clearinghouse.

Each physician/provider/supplier that uses 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.

Physicians/providers/suppliers should remember that they agreed to use sufficient security procedures (including compliance with all provisions of the HIPAA security regulations) to ensure that all transmissions of information are authorized and all beneficiary-specific data is protected from improper access. Acting on behalf of the beneficiary, physicians/providers/suppliers/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.

### ***Authenticating Data Elements for HIPAA 270/271 Eligibility Data***

Authenticating data elements for HIPAA 270/271 Eligibility Data must be provided by the inquirer (physician, provider, supplier, or other authorized third party) prior to the release of any beneficiary-specific eligibility information and must 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; and
- Date of birth.

### ***Medicare Beneficiary as First Source of Health Insurance Eligibility Information***

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

#### **Disclaimer**

This article was prepared as a service to the public and is not intended to grant rights or impose obligations. This article may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.

showing their health insurance coverage. This will not only help you determine who to bill for services rendered, but also provide you with 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. It is important to use the name as shown on the Medicare 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.

### ***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 the following:

- 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); and
- Determine proper billing.

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 physician/provider/supplier 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.

#### **Disclaimer**

This article was prepared as a service to the public and is not intended to grant rights or impose obligations. This article may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.

- You will promptly inform CMS or one of CMS's contractors (your carrier/DMERC/RHHI/FI) 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.

**Note:** Medicare health benefit beneficiary eligibility inquiries are monitored. Providers identified as demonstrating aberrant behavior (e.g., high inquiry error rate or high ratio of eligibility inquiries to claims submitted) may be contacted to verify proper use of the 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' Provisions*

Remember that a number of statutes provide for severe criminal and civil penalties for misuse of information, including:

#### **1. 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."

#### **2. 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.

#### **3. 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

#### **Disclaimer**

This article was prepared as a service to the public and is not intended to grant rights or impose obligations. This article may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.

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.

## Additional Information

---

CR5138, the official instructions issued to your Medicare FI, carrier, RHHI, and DMERC regarding this change, can be found at <http://www.cms.gov/Regulations-and-Guidance/Guidance/Transmittals/downloads/R991CP.pdf> on the CMS website. The revised section Chapter 31—ANSI X12N Formats Other than Claims or Remittance of the Medicare Claims Processing Manual is attached to CR5138.

If you have questions, please contact your Medicare FI, carrier, RHHI, or DMERC at their toll-free number, which may be found at <http://www.cms.gov/Research-Statistics-Data-and-Systems/Monitoring-Programs/provider-compliance-interactive-map/index.html> on the CMS website.

### Disclaimer

This article was prepared as a service to the public and is not intended to grant rights or impose obligations. This article may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations and other interpretive materials for a full and accurate statement of their contents.