



Related MLN Matters Article #: MM5138

Date Posted: June 29, 2006

Related CR #: 5138

Rules Governing Provider/Clearinghouse Protection of Medicare Beneficiary Eligibility Information

Key Words

MM5138, CR5138, R991CP, Provider, Clearinghouse, Protection, Eligibility, Information, Enrollment, EDI

Provider Types Affected

Physicians, providers, suppliers, and clearinghouses who bill Medicare fiscal intermediaries (FIs), carriers, regional home health intermediaries (RHHIs), durable medical equipment regional carriers (DMERCs), DME Medicare Administrative Contractors (DME MACs) 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

Key Points

- The effective date of the instruction is July 24, 2006.
- The implementation date is July 24, 2006.
- 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.)
- MLN Matters article MM5138 and related Change Request (CR) 5138 provide a reminder to physicians/providers/suppliers of the importance of protecting Medicare beneficiary information and to use it only for authorized purposes.
- MM5138 and CR5138 reiterate the responsibilities of users in obtaining, disseminating, and using beneficiary's Medicare eligibility data.

Key Points that Outline 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, DME MAC 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's last name (must match the name on the Medicare card);
 - Beneficiary's 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 the provider's first source of health insurance eligibility information. When scheduling a medical appointment for a Medicare beneficiary, a provider should remind the Medicare beneficiary to bring, on the day of their appointment, all health insurance cards showing their health insurance coverage.
- This will not only help providers determine who to bill for services rendered but also provide them 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 that providers use the name as shown on the Medicare card.
- If the beneficiary has Medicare coverage but does not have a Medicare Health Insurance card, providers should 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/coinsurance;
 - 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.

Note: 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, a provider will be responsible for the following:
 - Before requesting Medicare beneficiary eligibility information and at all times thereafter, providers will ensure sufficient security measures to associate a particular transaction with the particular employee.
 - Providers will cooperate with CMS or its agents in the event that CMS has a security concern with respect to any eligibility inquiry.
 - Providers will promptly inform CMS or one of CMS's contractors (carrier/DMERC/DME MAC/RHHI/FI) in the event they 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 a provider, or who has contacted them about treatment or service, or for whom they 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

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)

- The Department of Health and Human Services (DHHS) 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.

Important Links

<http://www.cms.hhs.gov/MLNMattersArticles/downloads/MM5138.pdf>

The official instructions (CR5138) issued to the provider’s Medicare FI, carrier, RHHI, DME MAC and DMERC regarding this change, can be found at

<http://www.cms.hhs.gov/Transmittals/downloads/R991CP.pdf> on the CMS web site.

The revised section Chapter 31—ANSI X12N Formats Other than Claims or Remittance of the Medicare Claims Processing Manual is attached to CR5138.

If providers/suppliers have questions, they may contact their Medicare FI, carrier, RHHI, DME MAC or DMERC at their toll-free number, which may be found at

<http://www.cms.hhs.gov/MLNProducts/downloads/CallCenterTollNumDirectory.zip> on the CMS web site.