10.3 – Medicare HIPAA Eligibility Transaction System Inquiries

Rules of Behavior

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 services. 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.*