Centers for Medicare & Medicaid Services (CMS)
7500 Security Blvd
Baltimore, MD 21244-1850

HIPAA Eligibility Transaction System/

HETS Inquiries Rules of Behavior

Version 1.4

August 2022

Document Number: HETS_Inquiries_Rules_of_Behavior_v1.4_Final_BESST_HETS

Contract Number: HHSM-500-2017-00039I

Table of Contents

List of Figures

No table of figures entries found.

List of Tables

1. HIPAA Eligibility Transaction System (HETS) 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. Provisions of the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 places restrictions on the disclosure of Medicare eligibility data. You should use the Medicare beneficiary eligibility transaction for conducting Medicare business only.

This document reiterates your responsibility in obtaining, disseminating, and using beneficiaries' Medicare eligibility data. It further explains the expectations for using HETS. You must accept these HETS Rules of Behavior in order to gain access to the system. If you violate these rules of behavior and/or other CMS data privacy and security rules, you could lose access and receive other penalties.

CMS monitors beneficiary eligibility inquiries. CMS may contact Providers, Clearinghouses, and/or Third Party Vendors (billing agents), herein referred to as "Submitters", identified as having aberrant behavior (e.g., high inquiry volume, high error rate, inappropriate use of specific Service Type Codes, using automated processes for sending large numbers of eligibility requests in a short period of time or high ratio of eligibility inquires to claims submitted) to verify and/or address improper use of the system or, when appropriate, refer them for investigation.

1.1 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 using HETS 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.

1.2 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.

- Sending beneficiary Medicare eligibility requests for the purpose of updating the beneficiary's records in a short timeframe using an automated process.

Submitters should only use Medicare eligibility data for the business of Medicare, such as preparing an accurate Medicare claim or determining eligibility for specific services. CMS expects submitters' authorized staff to use and disclose Protected Health Information (PHI) 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 HIPAA Privacy Rule also ensures protection for patients by limiting the ways that physicians, qualified non-physician practitioners, suppliers, hospitals and other provider covered entities can use a patient's personal medical information.

1.3 Accessing Beneficiary Eligibility Data: All Submitter Responsibilities

As a HETS 270/271 Submitter or an individual employed by a HETS 270/271 Submitter, you are responsible for the following:

- Before you request Medicare beneficiary eligibility information and at all times thereafter, you will ensure sufficient security measures are used, including user ID and passwords, to associate a particular transaction with the employee who initiated the eligibility inquiry, with respect to all 270s you submit to CMS.
- You will be fully accountable for all transactions you submit and will cooperate with CMS or its agents if CMS has a security concern with respect to any eligibility inquiry you submitted to CMS.
- Your organization will clearly divulge any offshore arrangements in Appendix E of the HETS Trading Partner Agreement (TPA).
- You will not purposefully manipulate or obfuscate your organization's IP address when submitting eligibility inquiries to CMS. CMS must be able to see the IP address from where the eligibility request originated.
- You will immediately inform CMS or one of CMS' contractors in the event you identify misuse of "individually identifiable" health information you accessed from the CMS database.
- You will immediately inform CMS or one of CMS' contractors in the event the identity or contact information of the Trading Partner Authorized Representative that appears on the HETS TPA changes. You will also agree to recertify your HETS access annually by resubmitting your HETS TPA after CMS notifies you to do so at a date of its choice. Failure to complete this recertification will result in a loss of access to HETS.
- You will immediately inform CMS or one of CMS' contractors in the event that you no longer meet any of the Rules of Behavior.
- You will immediately cease transmission of eligibility inquiries to CMS when you no longer meet any of the HETS Rules of Behavior.
- You must 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, lend, or otherwise transfer identification numbers and/or passwords.
    - Use CMS data files for private gain or to misrepresent yourself or CMS.
    - Browse or use CMS data files for unauthorized or illegal purposes.
    - Disclose CMS data that is not specifically authorized.

If you violate any of these security requirements, you could lose systems access privileges and/or face 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.

1.4 Clearinghouse Responsibilities

The Medicare Electronic Data Interchange (EDI) Enrollment process (https://www.cms.gov/Medicare/Billing/ElectronicBillingEDITrans/EnrollInEDI) provides for the collection of the information you need 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 agree to use sufficient security procedures (including compliance with all provisions of the HIPAA security regulations) to ensure that all data transmissions 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.

Per the EDI agreement, to receive access to eligibility data on behalf of Medicare Fee-For-Service (FFS) providers, a Clearinghouse Submitter must adhere to the following rules:

- The Clearinghouse 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.
- Each Medicare FFS provider that contracts with a Clearinghouse must sign a valid EDI Enrollment Form and be approved by a Medicare contractor before the provider can send eligibility data to the third party.
- Each Clearinghouse must sign a Trading Partner Agreement directly with CMS and/or one of CMS' contractors.
- The Clearinghouse must be able to associate each inquiry with the Medicare FFS provider or billing service making the inquiry. That is, for each inquiry a Clearinghouse makes, that vendor must be able to identify the Medicare FFS 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.
- The Clearinghouse will release eligibility data only to active Medicare FFS providers or their authorized billing agents for the purpose of preparing an accurate Medicare claim or determining eligibility for specific services. The Clearinghouse will not disclose information to anyone other than the Medicare FFS provider and/or supplier seeking to file a claim.

CMS will prohibit or suspend Clearinghouse access if there is a record of violation that would indicate that beneficiary data could be at risk of improper disclosure due to access the Clearinghouse approved.

1.5 Medicare FFS Provider/Supplier Responsibilities

Each Medicare FFS provider that submits/receives Medicare beneficiary eligibility data via EDI either directly to or from Medicare or through a Clearinghouse or Third Party Vendor must execute the EDI Enrollment.

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.

Per the EDI agreement, to receive access to Medicare beneficiary eligibility data, a Medicare FFS provider submitter must adhere to the following rules:

- You will submit an eligibility inquiry only if you are a valid, non-terminated Medicare FFS provider.
- Each eligibility inquiry will be limited to requests for Medicare beneficiary eligibility data with respect to a patient you are currently treating or serving, or who has contacted you about treatment or service, or for whom you have received a referral from a health care provider that is going to treat or serve that patient.

Appendix A. Revision History

Table 1 provides a summary of changes made to this document.

Table 1. Document Revision History

Version	Date	Description of Changes
1.1	7/21/2014	Significant modification of the document including content, formatting, and grammatical corrections throughout the document. Formalized document presentation including versioning and change control.
1.2	10/23/2015	Updated the following sections: • Introduction – added additional examples of aberrant behavior not tolerated by CMS • Section 2 – added an additional unauthorized behavior • Section 6.2 – added an additional unallowable Submitter behavior
1.3	01/27/2020	Updated URL in Section 4. Removed Section 6 from the previous version.
1.4	08/01/2022	Section 1.3 – updated the timeline for several statement from ‘promptly’ to ‘immediately.’ Added bullets 3 & 4 regarding offshore arrangements and originating IP addresses for inbound eligibility requests.