



Centers for Medicare & Medicaid Services (CMS)

7500 Security Blvd
Baltimore, MD 21244-1850

HIPAA Eligibility Transaction System (HETS) Inquiries Rules of Behavior

FINAL

Version: 1-2

Date of Last Revision: October 28, 2015

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 inquiries to claims submitted) to verify and/or address improper use of the system or, when appropriate, refer them for investigation.

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.

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.

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 in the event that CMS has a security concern with respect to any eligibility inquiry you submitted to CMS.
- You will promptly 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 promptly 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 Trading Partner Agreement (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 promptly 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.

4 Clearinghouse Responsibilities

The Medicare Electronic Data Interchange (EDI) Enrollment process (<http://www.cms.gov/Medicare/Billing/ElectronicBillingEDITrans/EnrollInEDI.html>) 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.

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.

6 HETS 270/271 Best Practices

CMS has compiled a list of HETS submitter “Dos” and “Don’ts” to provide additional guidance regarding HETS 270/271 best practices. CMS requires that all HETS 270/271 submitters read the best practices and review their own business practices to ensure that their organization is following these guidelines. CMS will contact submitters whose behavior is not consistent with these practices to determine the submitter’s action plan to improve.

In addition, review HETS 270/271 content information in Sections 7.2 - 7.19 of the HETS 270/271 Companion Guide online at:

<http://cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Downloads/HETS270271CompanionGuide5010.pdf>

HETS Submitters who use either the Support of Simple Object Access Protocol + Web Services Description Language envelope standards (SOAP) or Support of Hypertext Transfer Protocol/Multipurpose Internet Mail Extensions Multi-part envelope standards (MIME) Internet connection method should also review the HETS Submitter SOAP/MIME Connectivity Instructions online at:

<http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-InformationTechnology/HETSHelp/Downloads/HETS270271SOAPMIMEConnectivity.pdf>

6.1 HETS 270/271 Submitters should:

a) Transaction Content:

- Review CMS notifications of upcoming HETS 270/271 releases to ensure they are aware of planned system changes. HETS 270/271 typically has 3-5 releases per year that either require changes to the 270 request file or result in changes to the 271 response file. You should review the release notifications to understand the changes planned for HETS and incorporate appropriate changes into your eligibility system/product.
- Offer Medicare providers/suppliers the ability to employ alternate Medicare beneficiary search options. Version 5010A1 of HETS 270/271 supports three beneficiary search options. Medicare providers/suppliers should have the choice of selecting their search criteria based on data they have verified with the beneficiary. Refer to the HETS 270/271 Companion Guide for more information.
- Offer Medicare providers/suppliers the ability to select the Date(s) of Service for which they will submit the 270 eligibility request.
- Offer Medicare providers/suppliers the ability to select the specific Service Type Code(s) and/or HCPCS Code(s) they wish to send in the 270 eligibility request. The Service Type and HCPCS Codes that the HETS 270/271 supports appear in the HETS 270/271 Companion Guide. Publish updates to their Medicare provider/supplier customers when enhancements are made to the 271 response following HETS releases. Submitters should ensure that their customers understand that the Submitter is taking advantage of all of HETS' available capabilities and features.
- Modify their systems/products to display all of the information the HETS 271 response returns, including any applicable error messages. Submitters may choose to logically organize the information display or offer filters that allow Medicare providers/suppliers to focus on certain types of information – however, the Submitter should ensure that the provider/supplier has access to the full eligibility response.
- If applicable, ensure that you return an updated Medicare Health Insurance Claim Number (HICN, also known as a Medicare Number or Medicare Member ID) to the Medicare provider/supplier who requested eligibility data. If an eligibility request contains valid Medicare beneficiary data but has been submitted with an old, inactive HICN then HETS will return a 271 AAA Error response that also includes the new, active HICN for the same beneficiary. Submitters should ensure that they provide this corrected (or cross-referenced) HICN to the requesting Medicare provider/supplier. The Medicare

provider/supplier should update their records to ensure prompt processing of eligibility and claims files.

b) General Communication Protocol:

- Only request an open TCP/IP socket connection as necessary to support your active eligibility requests.
- Submit the 270 request immediately after successfully negotiating the TCP/IP socket. You should be as efficient as possible when using available sockets.
- Monitor the TCP/IP socket connection while connected to ensure that the socket remains open and viable. You should be able to determine if a socket has prematurely terminated for any reason.
- Submit only one transaction concurrently per TCP/IP socket. Transactions process linearly; submitting more than one transaction per socket concurrently results in additional transaction(s) queuing, delaying response time to the additional transactions.
- CMS recommends that high volume submitters send transactions asynchronously; that is, streaming multiple sequential requests via single TCP/IP socket connection. If you send transactions asynchronously, submit the next 270 request as soon as you receive the response to the previous request. Asynchronous submitters may open multiple TCP/IP sockets if necessary to support transaction volume during high volume periods.
- Limit your number of simultaneous TCP/IP connections to HETS 270/271. There are a finite number of available HETS sockets. You should be as efficient as possible when using available TCP/IP sockets; sending asynchronously improves socket efficiency.
- Close the TCP/IP socket immediately after you receive the last requested response. All submitters should forcefully terminate the TCP/IP socket connection when complete. HETS is configured to close idle connections, but only after a 5 second delay to see if additional requests will be sent. Submitters will greatly improve overall socket availability if they forcefully terminate all socket requests when complete.

c) SOAP/MIME Protocol:

- Obtain a SOAP- or MIME-specific HETS Submitter ID that allows the submitter to send eligibility inquiries to the HETS 270/271 application using SOAP or MIME. Submitters should not use other types of HETS Submitter IDs for SOAP or MIME requests without explicit instruction from CMS or CMS' Contractors.
- Obtain a HETS-recognized digital certificate for exchanging eligibility transactions via SOAP and MIME protocols and provide all necessary information to MCARE. You can find a list of HETS-recognized digital certificates within the HETS Submitter SOAP/MIME Connectivity Instruction document.

- Read and abide by the HETS Web Services Security Policy. Submitters are provided this policy as part of the on-boarding process.
- Send only one eligibility inquiry in a single SOAP or MIME request. The HETS 270/271 application does not support batch processing.
- Send a MIME attachment with only a (.txt) file extension. If an attachment with a file extension other than (.txt) is received, the transaction will be rejected.

6.2 HETS 270/271 Submitters should not:

a) Transaction Content:

- Submit eligibility requests simply for the purpose of updating a beneficiary record. 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.
- Ignore CMS notifications regarding updates to the HETS 270/271 application. The majority of releases involve changes to the 271 response. You should modify your systems/products to support HETS changes and return the data that CMS deems most relevant to Medicare providers/suppliers.
- Offer Medicare providers/suppliers fewer inquiry choices than HETS offers. HETS is ANSI X12N compliant, supporting multiple beneficiary search options, a wide range of Dates of Service, and a variety of Service Type Codes and/or HCPCS Codes.
- Require the Medicare provider/supplier to submit additional beneficiary details (e.g., gender or Middle Initial) beyond the minimum necessary data required as mandated by the HIPAA standards.

b) General Communication Protocol:

- Open a TCP/IP socket without an active eligibility request ready to be sent. You should not preemptively open sockets in anticipation of possibly needing to submit an eligibility request. You should also not submit requests to HETS solely for the purpose of determining the availability and/or status of the HETS system.
- Send more than one eligibility request concurrently per TCP/IP socket without waiting for a response. HETS processes transactions serially, even if more than one eligibility transaction is submitted at once on a socket. Transactions submitted during periods of high volume and corresponding long response times may cause the HETS system to reject a large number of these transactions.
- Submit duplicate eligibility requests in the same 24 hour period. The database HETS uses is updated once daily between 12:00 AM and 4:00 AM Eastern Time. Submitting a duplicate eligibility request within the 24 hour period of 4:00 AM to 11:59 PM will result in HETS returning an identical eligibility response.

c) SOAP/MIME Protocol:

- Send more than one eligibility inquiry in a single SOAP or MIME request.
- Send eligibility inquiries as attachments to SOAP requests.

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: <ul style="list-style-type: none"> - 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