

**Medicare HIPAA Eligibility Transaction System**  
**Trading Partner Agreement Submission**

---

PRA Disclosure Statement

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number. The valid OMB control number for this information collection is 0938-0960. The time required to complete this information collection is estimated to average 15 minutes per response, including the time to review instructions, search existing data resources, gather the data needed, and complete and review the information collection. If you have comments concerning the accuracy of the time estimate(s) or suggestions for improving this form, please write to: CMS, 7500 Security Boulevard, Attn: PRA Reports Clearance Officer, Mail Stop C4-26-05, Baltimore, Maryland 21244-1850.

**I. Background**

**A. Purpose of the Agreement**

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 Medicare beneficiary eligibility transaction is to be used for conducting Medicare business only.

In its administration of the Medicare FFS program, The Centers for Medicare & Medicaid Services (CMS) is a covered entity under the HIPAA rules. This Trading Partner Agreement serves to identify entities external to CMS that will exchange HIPAA compliant electronic transactions with CMS applications. The information collected will enable CMS and the Trading Partner to establish connectivity, define the data exchange requirements, and stipulate the responsibilities of the entities receiving CMS-supplied beneficiary eligibility information.

Connectivity to CMS eligibility systems is supported by use of the Extranet and/or the Internet. Eligibility information currently available on the Extranet is through the HIPAA Eligibility Transaction System (HETS). HETS supports the exchange of the HIPAA compliant 270 Eligibility Inquiry and 271 Eligibility Response. The eligibility application currently available on the Internet is the data equivalent of the 270/271 exchange.

Entities that wish to submit 270 inquiries to Medicare via HETS on a real-time basis (hereinafter, "Submitter" or "Submitters") will use the AT&T communication Extranet (the Medicare Data Communication Network, or MDCN). This Extranet is a secure closed private network currently used to transmit data between Medicare FFS contractors and CMS, as well as for transmission of electronic transactions between

CMS and providers or clearinghouses. In order to access the MDCN, Submitters must obtain the necessary AGNS connectivity from an AT&T reseller.

As a covered entity in making the disclosures of information in the 271 response transaction, CMS is required to verify the identity of the individual requesting the Protected Health Information and the individual's authority to have access to that information. Federal law requires that CMS take precautions to minimize security risks to the federal information systems. Accordingly, CMS is requiring that trading partners who wish to conduct the 270/271 transaction on a real-time basis provide certain assurances as a condition of receiving access to the Medicare data.

## **B. Authorized Uses**

Medicare eligibility data are only to be used for Medicare business done on behalf of Medicare providers, including preparing accurate Medicare claims or determining eligibility for specific services. Authorized requests for Medicare beneficiary eligibility information are listed below:

- **After screening** the patient to determine Medicare eligibility, 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, Part C plan (Medicare Advantage), or Part D plan.
- Determine proper billing
- Checking eligibility for a Medicare beneficiary currently being treated or serviced or who has contacted a Medicare provider about treatment or service, or for whom a Medicare provider has received a referral from a health care provider that has treated or served that patient.

## **C. Criminal Penalties**

CMS monitors beneficiary eligibility inquiries. Submitters demonstrating behavior that suggests improper use of the data (e.g., high inquiry error rate or, for provider submitters, high ratio of eligibility inquiries to claims submitted) may be suspended, put on a corrective action plan (CAP) or, when appropriate, be referred for investigation. Criminal penalties could be imposed for continued aberrant behavior.

### **PENALTIES FOR FALSIFYING INFORMATION ON, WRONGFUL OBTAINING OF INFORMATION THROUGH, AND WRONGFUL DISCLOSURE OF INFORMATION OBTAINED PURSUANT TO, THE TRADING PARTNER AGREEMENT FOR SUBMISSION OF 270s TO MEDICARE ON A REAL-TIME BASIS.**

#### **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.

18 U.S.C. 1001 authorizes criminal penalties against an individual who in any matter within the jurisdiction of any department or agency of the United States knowingly and willfully falsifies, conceals, or covers up by any trick, scheme, or device, a material fact, or makes any false, fictitious or fraudulent statements or representations, or makes any false writing or document knowing the same to contain any false, fictitious or fraudulent statement or entry. Individual offenders are subject to fines of up to \$250,000 and imprisonment for up to 5 years. Offenders that are organizations are subject to fines of up to \$500,000. 18 U.S.C. 3571(d) also authorizes fines of up to twice the gross gain derived by the offender if it is greater than the amount specifically authorized by the sentencing statute.

## **II. Assurances**

**Provision by CMS of access to the HETS Extranet is subject to Submitter's agreement and assurances as set forth below. Access to HETS may be terminated by CMS, without prior notice to the Submitter, in the event that CMS determines based on information from the Submitter or otherwise, that Submitter has not complied with one or more of the assurances hereafter provided by Submitter.**

In consideration of the foregoing, and in order to obtain access to HETS on a real-time basis, the Submitter hereby agrees and assures, by checking the left-hand boxes, as appropriate, as follows:

**All Submitters:**

- Submitter will not make any disclosure of CMS data that is not specifically authorized; the Submitter has read and fully understands the authorized disclosures as outlined in this document.
- Before submitting any 270s and at all times thereafter, submitter will ensure that it provides sufficient security measures, including user ID and passwords, to associate a particular 270 with the particular employee who initiated the eligibility inquiry, with respect to all 270s that it submits to CMS.
- Submitter is fully accountable for all transactions submitted and will cooperate with CMS or its agents in the event that CMS has a security concern with respect to any 270 submitted by Submitter to CMS.
- Submitter will promptly inform the HETS Help Desk, using such means as the HETS Help Desk may identify, in the event the identity or contact information of Submitter's Authorized Representative changes, or if any of the assurances herein provided are no longer met.
- Submitter will immediately cease transmission of 270 to CMS at such time that any of the assurances herein provided are no longer met.
- Submitter will not disclose, lend, or otherwise transfer 270/271 transaction identification numbers and/or password to someone else.
- Submitter will not use CMS data files for private gain or to misrepresent yourself or CMS.
- Submitter will not browse or use CMS data files for unauthorized or illegal purposes

**All Clearinghouse Submitters:**

Along with the previous provisions for all submitters, all clearinghouse submitters must attest to:

- Clearinghouse will release eligibility data only to active Medicare providers or their authorized billing agents for the purpose of preparing an accurate Medicare claim or determining eligibility for specific services. Clearinghouse will not disclose information to anyone other than the Medicare provider and/or supplier, seeking to file a claim.
- Clearinghouse will be able to associate each inquiry with the provider or billing service making the inquiry. That is, for each inquiry submitted, the clearinghouse will be able to identify the provider making the request for beneficiary information and be able to assure that eligibility responses are routed only to the provider that originated each request.
- Upon request from the HETS Help Desk, clearinghouse will submit listings of all providers for which it is submitting requests for beneficiary information.

- Clearinghouse access will be prohibited or suspended if CMS auditing shows violation of this agreement putting beneficiary data at risk of improper disclosure.
- Clearinghouse will 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 Clearinghouse submits a 270 that has been prepared by a provider/supplier utilizing clearinghouse services, the Clearinghouse will be 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.

**All Provider Submitters:**

Along with the previous provisions for all submitters, all provider submitters must attest to:

- 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.
- 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 request the 270 transaction only if you are a valid non-terminated Medicare provider.

**Attestation:**

The Authorized Representative whose name is supplied below is authorized to bind Submitter to the undertakings in this agreement. By completing the section below you are agreeing that your organization will be in compliance with the provisions listed above.

(\* indicates required field)

\* Authorized Representative:

\* Authorized Representative's Title:

\* Authorized Representative's Contact Information:

\* (Phone):

\* (E-mail address):

Secondary Authorized Representative:

Secondary Authorized Representative's Title:

Secondary Authorized Representative's Contact Information:

(Phone):

(E-mail address):

\* Submitter's Name:

\* Medicare Provider Number/NPI:

\* Legal Business Name:

\* DBA/Medicare Provider's Name

\* Billing Address (Street or P.O. Box):

\* City:

\* State:

\* Zip Code:

\* Physical Address (May not enter a P.O. Box):

\* City:

\* State:

\* Zip Code: