



---

MEDICARE HIPAA ELIGIBILITY TRANSACTION  
SYSTEM (HETS) TRADING PARTNER  
AGREEMENT (TPA)

---

CMS-Version 4.1



## TABLE OF CONTENTS

<b>Form Instructions .....</b>	<b>1</b>
<b>CENTERS FOR MEDICARE &amp; MEDICAID SERVICES (CMS) TRADING PARTNER AGREEMENT .....</b>	<b>1</b>
I. BACKGROUND .....	2
II. AUTHORIZED USES .....	2
III. SYSTEM INTEGRITY .....	2
IV. CONNECTIVITY .....	3
V. ASSURANCES .....	3
<b>APPENDIX A – REFERENCES – Required .....</b>	<b>6</b>
<b>APPENDIX B - INFORMATION REQUIRED TO REQUEST ACCESS TO THE HIPAA ELIGIBILITY TRANSACTION SYSTEM – Required .....</b>	<b>7</b>
<b>APPENDIX C – CONNECTIVITY – Required .....</b>	<b>8</b>
<b>APPENDIX D – DSH – Situational .....</b>	<b>9</b>
<b>APPENDIX E – OFFSHORE DATA PROTECTION – Situational .....</b>	<b>10</b>

---

## FORM INSTRUCTIONS

---

Please check one (1) box to indicate the type of Agreement being submitted:

- Initial Trading Partner Application
- Annual TPA Recertification
- Other TPA Update

---

### CENTERS FOR MEDICARE & MEDICAID SERVICES (CMS) TRADING PARTNER AGREEMENT

---

For Use of the Medicare HIPAA Eligibility Transaction System (HETS) to Conduct the Health Care Eligibility Benefit Inquiry and Response transactions.

This Trading Partner Agreement (“Agreement”) is made on [REDACTED] between the Centers for Medicare & Medicaid Services and [REDACTED].

The Trading Partner (also known as the Submitter), intends to conduct eligibility transactions with CMS in electronic form. Both parties acknowledge and agree that the privacy and security of data held by or exchanged between them is of utmost priority. Each party agrees to take all steps reasonably necessary to ensure that all electronic transactions between them conform to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and regulations promulgated thereunder. Unless defined herein, all terms have the same meaning as in the regulations promulgated to implement the Administrative Simplification provisions of HIPAA at 45 CFR Parts 160-164.

#### **PAPERWORK REDUCTION ACT (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 expires January 31, 2023. 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. Please do not send applications, claims, payments, medical records or any documents containing sensitive information to the PRA Reports Clearance Office. Please note that any correspondence not pertaining to the information collection burden approved under the associated OMB control number listed on this form will not be reviewed, forwarded, or retained. If you have questions or concerns regarding where to submit your documents, please contact the MCARE Help Desk at 1-866-324-7315 or [mcare@cms.hhs.gov](mailto:mcare@cms.hhs.gov).

---

## I. BACKGROUND

---

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 (Privacy Act) and HIPAA. The Medicare beneficiary eligibility transaction is to be used for conducting Medicare business only.

In its administration of the Medicare Fee-For-Service (FFS) program, 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 software applications. The HIPAA Eligibility Transaction System (HETS) supports the ASC X12 270/271. The information collected by the HETS system 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.

---

## II. AUTHORIZED USES

---

Medicare eligibility data are only to be used for Medicare business done on behalf of Medicare FFS providers, including preparing accurate Medicare claims or determining eligibility for specific services. Authorized and unauthorized uses are provided in the HETS Rules of Behavior referenced in Appendix A, available on the CMS website, and incorporated by reference herein.

Trading Partners cannot electronically store or reuse Medicare beneficiary protected health information (PHI) obtained from HETS, except for the following purposes expressly authorized by CMS:

- To maintain an historical account of processing activity
- In accordance with procedures (e.g., routine system backups) to support data restoration in the event of a disaster
- To update patient account records in the record management system of the FFS Medicare provider requesting the data

Any data storage by Trading Partner or its Business Associates, as defined by 45 CFR §160.103, must be compliant with the HETS Rules of Behavior.

---

## III. SYSTEM INTEGRITY

---

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, placed on a corrective action plan (CAP) or, when appropriate, be referred for investigation. Civil and/or criminal enforcement may be pursued where appropriate.

### 1. HIPAA Violation

The U.S. Department of Health and Human Services (HHS) may impose civil money penalties on a covered entity of up to \$50,000 for failure to comply with a provision in the Privacy, Security, and Breach Notification Rules, with maximum annual limits for violations of identical provisions, which are set forth at 42 U.S.C. 1320d-5(a). A person who knowingly obtains or discloses individually identifiable health information in violation of HIPAA faces criminal

penalties ranging from \$50,000, up to one-year imprisonment, or both, to, in circumstances where the wrongful conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, up to \$250,000, up to ten years imprisonment, or both Criminal enforcement is conducted by the Department of Justice.

## 2. Civil False Claims Act Violation and Criminal Violations

The False Claims Act, 31 U.S.C. §§ 3729-3733, provides that one who knowingly submits, or causes another person or entity to submit, false claims for payment of government funds is liable for three times the government's damages plus civil penalties of \$11,181 to \$22,363 per false claim (note that the civil penalty amounts are subject to an inflation adjustment; these were the amounts for calendar year 2018).

Various federal criminal provisions authorize imposition of criminal penalties, including fines and imprisonment, against individuals who, with respect to Government or health care benefit programs, engage in conduct including, but not limited to, falsifying or concealing a material fact or making materially false, fictitious, or fraudulent statement.

---

## IV. CONNECTIVITY

---

Connectivity to CMS eligibility systems is supported by the use of the Extranet and/or the Internet. A Trading Partner may submit a request using the 270 standard to HETS using Transmission Control/Internet Protocol (TCP/IP) for extranet access or Simple Object Access Protocol (SOAP) + Web Services Description Language (WSDL) or Hypertext Transfer Protocol (HTTP)/Multipart Internet Mail Extensions (MIME) Multipart communication protocols for public Internet access. For additional information, including connectivity options, refer to the HETS Rules of Behavior. All Submitters shall submit the information required in Appendix B to request connectivity and be compliant with the guidance referenced in Appendix A.

---

## V. ASSURANCES

---

Provision by CMS of access to HETS, both Extranet and Internet, is subject to Submitter's 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 the HETS system, the Submitter hereby agrees and assures as follows:

No.	Assurance	Agreement
1.	Submitter agrees to abide by all applicable federal laws, regulations, and guidance governing access to, and use and disclosure of, CMS data, Protected Health Information (PHI) as defined in 45 CFR §160.103, and Personally Identifiable Information (PII) as defined in OMB Memorandum M-07-16 (May 22, 2007) and understands that individuals or entities may be subject to civil and/or criminal penalties for failing to abide by such provisions.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree

---

No.	Assurance	Agreement
2.	Before initiating any transmission in HIPAA standard 270/271 transaction format, and thereafter through the term of this Agreement, the Trading Partner will cooperate with CMS and any contractors representing CMS in testing of the transmission and processing systems used in connection with CMS as deemed appropriate to ensure the accuracy, timeliness, completeness, and security of each data transmission.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree
3.	Submitter will take reasonable care to ensure that the information submitted in each electronic transaction is timely, complete, accurate, and secure, and will take reasonable precautions to prevent unauthorized access of the party's transmission and processing systems. The Submitter will ensure that each electronic transaction submitted to CMS conforms with the requirements applicable to the transaction.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree
4.	Every Submitter must be an active enrolled Medicare provider or a Business Associate working on behalf of active enrolled Medicare provider(s) before any submission of electronic transactions is allowed. The Submitter agrees to notify CMS when its relationship with a Medicare provider both begins and terminates. Business Associate Submitters are responsible for providing current information about the provider(s) for whom they are submitting transactions in accordance with the HETS Rules of Behavior. CMS reserves the right to confirm the status of a Business Associate relationship with a provider directly.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree
5.	Submitters shall notify CMS of a change in Business Associate representation consistent with the HETS Rules of Behavior.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree
6.	All Submitters must comply with and follow the HETS Rules of Behavior, referenced in Appendix A, in all areas not specifically listed in this Agreement, including how to address making changes to the information supplied in Appendix B.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree
7.	This Agreement shall take effect and be binding on the Trading Partner and CMS when signed by the Trading Partner and reviewed and signed by an authorized CMS representative.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree
8.	Termination or expiration of this Agreement or any other contract between the parties does not relieve either party of its obligations under this Agreement and under federal and state laws and regulations pertaining to the privacy and security of PHI and PII, nor its obligations regarding the confidentiality of CMS proprietary information.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree
9.	Submitters who perform Medicare work offshore (any location outside of the United States where U.S. law is non-binding) must attest that safeguards to protect Medicare Beneficiary Information are actively enforced. Any Submitters who perform work or either directly or indirectly employ offshore labor must attest to the terms specified in Appendix E. Submitters who do not perform any Medicare work offshore (or directly or indirectly employ any offshore labor should mark this assurance as 'Not Applicable.'	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree <input type="checkbox"/> Not Applicable

The Authorized Representative whose name is supplied below is authorized to bind the Trading Partner as a HETS Submitter to the undertakings of this Agreement. By completing the section below, you are agreeing that your organization will be in compliance with the provisions of this Agreement.

Trading Partner Authorized Representative Signature	Title
Printed Name of Trading Partner Authorized Signer	Date Signed
Telephone Number	E-Mail Address

---

## **APPENDIX A – REFERENCES – REQUIRED**

---

### **HETS Rules of Behavior**

This document details the Submitter's responsibilities in obtaining, disseminating, and using beneficiary's Medicare eligibility data. It further explains the expectations for using HETS. Compliance with these HETS Rules of Behavior is necessary in order to gain and maintain continued access to the system.

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

### **HETS Authorized Representative Roles and Responsibilities**

This document details the Authorized Representatives HETS roles and responsibilities. It is written confirmation that the Submitter's Authorized Representative understands his/her responsibility for the organization's use of HETS and compliance with the HETS Rules of Behavior.

<https://www.cms.gov/files/document/tpaarroleresponsibilities.pdf>



---

**APPENDIX B - INFORMATION REQUIRED TO REQUEST ACCESS TO THE HIPAA  
ELIGIBILITY TRANSACTION SYSTEM – REQUIRED**

---

(fields marked with \* are optional, all others are required)

**Submitter Organization Security Officer Contact Information (Optional):**

*Name: (Optional)	*Title: (Optional)
*Telephone number: (Optional)	*E-mail address: (Optional)

**Submitter Organization’s Information:**

Submitter Organization Name:		Submitter Organization Legal Business Name:	
Submitter Organization Billing Address:			
City	State	Zip Code	
Submitter Organization Physical Address:			
City	State	Zip Code	
Submitter Organization Technical Representative Name:			
Submitter Organization Technical Representative Telephone Number:		Submitter Organization Technical Representative E-mail Address:	
<p>CMS requires only one NPI from an active/valid enrolled Medicare provider(s) on this form. In accordance with item 4 in the Assurances section of the Agreement, submitter organization must later share any/all additional NPIs with CMS.</p>			
Medicare Provider’s Name:		Medicare Provider’s NPI:	

---

**APPENDIX C – CONNECTIVITY – REQUIRED**

---

Please indicate the type of connectivity used by the Trading Partner.

Extranet:	<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, Name of Network Service Vendor (NSV) used	
Internet:	<input type="checkbox"/> Yes <input type="checkbox"/> No
If yes, Message Envelope Used	<input type="checkbox"/> SOAP + WSDL <input type="checkbox"/> HTTP MIME Multipart

Trading Partner IP Address (es) for SOAP/MIME transaction (Note: If sending multiple IP addresses, please use a Classless Inter-Domain Routing [CIDR] notation, i.e., 192.0.1.0/24)

IP Address(es):	
X.509 Digital Certificate Issuer Name:	
X.509 Digital Certificate Type:	
X.509 Digital Certificate Serial Number:	

Note: If using SOAP + WSDL or HTTP MIME Multipart, applicants must send a copy of their organization's public x.509 digital certificate. The Trading Partner Agreement will not be processed without a copy of the public digital certificate.

---

## APPENDIX D – DSH – SITUATIONAL

---

For Disproportionate Share Hospital (DSH) Information Trading Partners:

CMS developed a limited view of the HIPAA Eligibility Transaction System (HETS) to allow hospitals that receive Medicare Disproportionate Share Hospital (DSH) payments to view Medicare enrollment information for their hospital inpatients. This data assists hospitals when verifying CMS' determination of the hospital's SSI ratio (i.e., the total number of Medicare days compared to the number of Medicare/SSI days). This information may be disclosed to Medicare HETS DSH Trading Partners under routine use of the 'Medicare Provider Analysis and Review (MEDPAR), HHS/CMS/OIS, 09-70-0514' Privacy Act system of records, published at 71 Fed. Reg. 17470 (April 06, 2006).

Eligible Trading Partners must request a separate DSH Submitter ID in order to utilize this view.

Specify the type of HETS Submitter ID(s) being requested:

DSH view only     DSH view and standard HETS 270/271

DSH Hospital NPI(s):

---

**APPENDIX E – OFFSHORE DATA PROTECTION – SITUATIONAL (IF YOU HAVE OFFSHORE ARRANGEMENT)**

---

**Offshore Data Protection Safeguards**

The Authorized Representative must positively affirm that all of the following safeguards are actively in place.

**Attestation of Safeguards to Protect Beneficiary Information Offshore**

No.	Assurance	Agreement
1.	Offshore arrangement has policies and procedures in place to ensure the privacy and security of Medicare beneficiary Protected Health Information (PHI), Personal Identifiable information (PII), and confidentiality of CMS proprietary information.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree
2.	Offshore arrangement prohibits access to Medicare data not associated with the offshore agreement.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree
3.	Offshore arrangement has policies and procedures in place that allow for immediate termination of the offshore work upon discovery of a significant security breach.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree
4.	Offshore arrangement will take reasonable precautions to prevent unauthorized access to the parties' transmission and processing systems.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree
5.	Offshore arrangement must comply with and follow HETS Rules of Behavior referenced in Appendix A.	<input type="checkbox"/> Agree <input type="checkbox"/> Disagree

The Authorized Representative named below must be authorized to attest to the Offshore Data Protection Safeguards Appendix E of the HETS Trading Partner Agreement. CMS requires applicants to complete all of the fields below, including signature. By completing and signing the section below, the Authorized Representative is agreeing that the organization will be in compliance with the provisions of this section.

Offshore Work Site Organization Name*	Offshore Work Site Organization Address including Country Name*	Offshore Work Site Organization Originating IP Address(es)*
Trading Partner Authorized Representative Signature		Title
Printed Name of Trading Partner Authorized Signer		Date Signed
Telephone Number		E-Mail Address

\*if multiple Organizations, then provide all  
 Note: Enter each/every Offshore Work Site's non-US Originating IP Address(es)