

Supporting Statement- Part A

The HIPAA Eligibility Transaction System (HETS) (CMS-10157; OMB 0938-0960)

Background

CMS created the HIPAA (Health Insurance Portability and Accountability Act of 1996) Eligibility Transaction System (HETS) to provide HIPAA Accredited Standards Committee X12 270/271 health care eligibility inquiries (270) and responses (271) on a real-time basis. HETS allows health care providers or their designees to check Medicare beneficiary eligibility data in real-time. They use HETS to prepare accurate Medicare claims, determine beneficiary liability, or check eligibility for specific services. HETS allows users to submit HIPAA compliant 270 eligibility request over a secure connection and receive 271 responses in real-time. In creating the HETS system, federal law requires that CMS take precautions to minimize the security risk to federal information systems. Accordingly, CMS requires that trading partners who wish to connect to the HETS 270/271 system via the CMS Extranet and/or Internet to agree to the HETS Rules of Behavior and the HETS Authorized Representative Roles and Responsibilities terms as a condition of receiving Medicare eligibility information. Applicants complete the entire Trading Partner Agreement form to indicate agreement with CMS trading partner terms and provide sufficient information to establish connectivity to the service and assure that those entities that access the Medicare eligibility information are aware of applicable provisions and penalties for the misuse of information.

The Centers for Medicare and Medicaid Services (CMS) is requesting the Office of Management and Budget (OMB) approve revisions to the currently approved HETS Trading Partner Agreement form. The revisions ensure it aligns with federal plain language guidelines.

We updated the Trading Partner Agreement to:

- Revise language throughout the document to align with federal plain language guidelines
- Remove language from Appendix D related to Disproportionate Share Hospitals (DSH)
- Add a check box for the Trading Partner Authorized Representative to acknowledge the revised HETS Rules of Behavior
- Add a check box for the Trading Partner Authorized Representative to acknowledge the HETS Authorized Representative (AR) Roles and Responsibilities
- Add a check box for the Training Partner Authorized Representative to acknowledge the offshore data protection safeguards (when applicable)
- Add a check box to ensure that the trading Partner Authorized Representative include the originating IP address on every transaction to HETS

We also removed all Appendix D questions and content related to DSH. We don't need to collect this information anymore because HETS users can't use the DSH view in HETS. DSH used a health insurance claim number (HICN)-based approach, but in 2020, CMS transitioned from HICNs to Medicare Beneficiary Identifiers (MBIs), making the DSH view obsolete. Lastly, we added 3 places for the respondent to acknowledge they'll adhere to CMS's safeguards to protect beneficiary information shared with them; these areas include:

- HETS Rules of Behavior (Appendix A)
- HETS Authorized Representative Roles and Responsibilities (Appendix A)
- Offshore Data Protection Safeguards, when applicable (Appendix D, formerly Appendix E)
- To include the originating IP address on every transaction to HETS

A. Justification

The TPA needed to be updated to align with Federal guidelines of plain language along with removal of the DSH section in Appendix D as eligibility requests using the HICN based is no longer available to be used because CMS mandated the use of MBIs for all eligibility requests. To safeguard the beneficiaries PHI/PII data, added acknowledgements by respondents for HETS rules of behavior, Authorized Representative Roles and Responsibilities, offshore data protection and to include originating IP addresses for all eligibility requests.

1. Need and Legal Basis

HIPAA regulations require covered entities to verify the identity of the person requesting PHI and the person's authority to have access to that information. Under the HIPAA Security rules, covered entities, regardless of their size, are required under 45 CFR Subtitle A, Subpart C 164.312(a)(2)(i) to "assign a unique name and/or number for identifying and tracking user identity." A 'user' is defined in 164.304 as a "person or entity with authorized access". Accordingly, the HIPAA Security rule requires covered entities to assign a unique name and/or number to each employee or workforce member who uses a system that receives, maintains, or transmits electronic protected health information (PHI) so that system access and activity can be identified and tracked by user. This includes workforce members within small or large provider offices, health plans, group health plans, and clearinghouses.

Federal law requires that CMS take precautions to minimize the security risk to the federal information system. Federal Information Processing Standards Publication (FIPS PUB) 1() 1-2 Paragraph 11.7- Security and Authentication states that: "Agencies shall employ risk management techniques to determine the appropriate mix of security controls needed to protect specific data and systems. The selection of controls shall take into account procedures required under applicable laws and regulations." Accordingly, CMS requires that entities who wish to connect to the HETS application via the CMS Extranet and/or Internet are uniquely identified. CMS is required to verify the identity of the person requesting the PHI and the person's authority to have access to Medicare eligibility information. Furthermore, CMS requires that trading partners who wish to conduct eligibility transactions on a real-time basis with CMS provide certain assurances as a condition of receiving access to the Medicare eligibility information for the purpose of conducting real-time 270/271 inquiry/response transactions.

2. Information Users

CMS uses the Trading Partner Agreement Form to capture certain information whereby a person certifies that they are fully aware of all penalties related to the use of PHI and their access to this data from the HETS application. The information is an attestation by the authorized representative of an entity that wishes to access the Medicare eligibility information to conduct real-time eligibility transactions. The authorized representative is a person responsible for business decisions on behalf of the Organization who is submitting the access request. The data captured includes the authorized representative's name, title contact number and

the name of the submitting entity. Other data captured is the submitter's National Provider Identifier, business name, billing address, physical address, and telephone number.

The Trading Partner Agreement Form is also used by CMS to capture certain information whereby a person identifies the particular connectivity protocol that they will use to connect to CMS and specific organization information which is reviewed and authorized prior to the access being granted.

3. Use of Information Technology

CMS allows public access to the HETS 270/271 application via the CMS Extranet and Internet to offer real-time eligibility inquiries (270) and responses (271) in an electronic format as a method for health care providers to get beneficiary eligibility using a secure network connection. The Trading Partner Agreement Form is available on the CMS website. When CMS gets a completed form, it's stored in the HETS Program Jira ticket system which is hosted in the CMS/AWS enclave. Responders must complete the Trading Partner Agreement Form before getting access to the CMS Extranet or Internet. Maintenance on the TPA form includes review, edits and possible updates of the content are managed by CMS.

CMS reserves the right to update the Trading Partner Agreement Form with non-substantive changes like:

- updating or adding URLs
- clarifying requested information
- Changes in contact information for the Medicare Customer Assistance Regarding Eligibility (MCARE) Help Desk

4. Duplication of Efforts

Existing submitters must resubmit a new copy of the Trading Partner Agreement Form annually to ensure CMS has accurate information.

New submitters haven't submitted a Trading Partner Agreement Form to connect to the HETS 270/271 application via the CMS Extranet or Internet to access Medicare eligibility information to conduct HIPAA transactions.

5. Small Businesses

There will be minimal impact on small businesses as the length of time to read, complete, and submit the Trading Partner Agreement Form is typically less than fifteen minutes.

6. Less Frequent Collection

This information will be collected annually for entities who want to connect to the CMS Extranet or Internet to conduct real-time eligibility transactions. Information submitted on the TPA helps CMS to only allow

entities who needs access to beneficiaries Medicare eligibility data. The information submitted on the TPA helps to protect beneficiaries' data as per the CMS security guidelines.

If entities will not provide this information, CMS has no way of knowing who is legally authorized to use CMS HETS application and whether these entities are agreeing to HETS rules of behavior, Authorized official Roles and Responsibilities, their acknowledgement to protect the CMS data and who to contact when needed.

7. Special Circumstances

There are no special circumstances that would require an information collection to be conducted in a manner that requires respondents to:

- Report information to the agency more often than quarterly
- Prepare a written response to a collection of information in fewer than 30 days after receipt of it
- Submit more than an original and two copies of any document
- Retain records, other than health, medical, government contract, grant-in-aid, or tax records for more than three years
- Collect data in connection with a statistical survey that is not designed to produce valid and reliable results that can be generalized to the universe of study
- Use a statistical data classification that has not been reviewed and approved by OMB
- Include a pledge of confidentiality that is not supported by authority established in statute or regulation that is not supported by disclosure and data security policies that are consistent with the pledge, or which unnecessarily impedes sharing of data with other agencies for compatible confidential use
- Submit proprietary trade secret, or other confidential information unless the agency can demonstrate that it has instituted procedures to protect the information's confidentiality to the extent permitted by law

8. Federal Register/Outside Consultation

The 60-day Federal Register Notice (89 FR) published to the Federal Register TBD.

9. Payments/Gifts to Respondents

There are no payments or gifts to respondents.

10. Confidentiality

The information collected will be gathered and used solely by CMS. The data will not be shared with any outside organizations.

11. Sensitive Questions

There are no sensitive questions on the Trading Partner Agreement Form.

12. Burden Estimates (Hours & Wages)

CMS currently has agreements in place with approximately 200 trading partners. In the future we anticipate that the provider community will continue to request access to Medicare eligibility information, but we don't anticipate the total number of agreements to exceed one thousand at any given time. We also don't anticipate a major influx of applications because of this proposed version, and any increase will come over a gradual period.

This form has about 25 data collection items like Submitter name, Security official name/contact information, National Provider ID etc., and some of the items are only Yes and No answers. Based on the information that we gathered in the last two years, we estimate that it should not take more than 15 minutes to read, execute and submit this TPA. The total burden is estimated to be 250 hours.

Max number of Users (estimated-annually) who will use and submit this form in a year=1000
 Total time to read/execute/Submit this form=15 min.
 Total time (estimated-annually) = 1000*15=15000 min. =250 hrs. Total burden (estimated) =250 hours.

Wage/Cost Estimates

Occupation Title	Occupation Code	Median Hourly Wage (\$/hr)	Fringe Benefit (\$/hr)	Adjusted Hourly Wage (\$/hr)
Computer Systems Analysts	15-1211	\$53.42	\$53.42	\$106.84

These Agreements are completed by Computer Systems Analysts. Based on the most recent Bureau of Labor and Statistics Occupational and Employment Data (May 2023) http://www.bls.gov/oes/current/oes_md.htm for Category 15-1211 (Computer Systems Analysts), the median hourly wage for this profession is \$53.42 We have added 100% of the median hourly wage to account for fringe and overhead benefits, which calculates to \$106.84(\$53.42 + 53.42). We estimate the total annual cost to be \$24,950.00 (250 hours x \$99.80/hour).

	# Respondent	Cost per hour*	Time per submission	Total Burden Hours	Total Cost
TOTAL	1000	\$106.84	0.25	250	\$26,710.00

13. Capital Costs

There are no capital costs to the respondents.

14. Cost to Federal Government.

We estimate it will cost the Federal Government \$50,000 to publish the Trading Partner Agreement form on the CMS website, receive, review, and store the completed forms. We estimate we'll get Trading Partner Agreement Forms from 1,000 respondents at a cost of \$50 each (1,000*\$50 = \$50,000).

15. Changes to Burden

The TPA is updated to align with Federal guidelines of plain language along with removal Appendix-D (DSH section) and added acknowledgements by respondents for HETS rules of behavior, Authorized Representative Roles and Responsibilities, offshore data protection and to include originating IP addresses for all eligibility requests. These changes do not increase or decrease the burden. But there is a change in hourly wages of the computer system analysts who complete this form, we estimate the annual cost burden will increase from \$23,805 to \$26,710 (a difference of \$2905.00).

16. Publication/Tabulation Dates

No publication or tabulation of data expected.

17. Expiration Date

The expiration date will be displayed within the PRA disclosure statement of the TPA.

18. Certification Statement

There are no exceptions to the certification statement.