CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES
OFFICE OF TECHNOLOGY SOLUTIONS

HETS 270/271 Frequently Asked Questions (FAQ)

Questions	Answers
What is HETS and how do I get connected to use this system?	The HIPAA Eligibility Transaction System (HETS) is intended to allow the release of eligibility data to Medicare providers or their authorized billing agents for the purpose of preparing an accurate Medicare claim, determining beneficiary liability, or determining eligibility for specific services. Such information may not be disclosed to anyone other than the provider, supplier, or beneficiary for whom a claim is filed. The information included in the 271 response is not intended to provide a complete representation of all benefits, but rather to address the status of eligibility (active or inactive) and patient financial responsibility for Medicare Part A and Part B. The data included in a 271 response file is to be considered true and accurate only at the particular time of the transaction. The HETS 270/271 application provides access to Medicare Beneficiary eligibility data in a real-time environment. In real-time mode, the Trading Partner transmits a 270 request and remains connected while the receiver processes the transaction and returns a 271 response. Providers, Clearinghouses, and/or Third Party Vendors, herein referred to as "Trading Partners", may initiate a real-time 270 eligibility request to query coverage information from Medicare on patients for whom services are scheduled or have already been delivered. Please refer to the HETSHelp 'How To Get Connected' page on the cms.gov website for additional information on how to obtain a connection to, and then apply for, HETS access. Please contact the Help Desk if you have any questions. https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/HowtoGetConnectedHETS270271.html
How do I sign up for HETS?	In order to obtain access to the HETS 270/271 application, a submitter needs to complete a Trading Partner Agreement (TPA). Please refer to the HETSHelp 'How To Get Connected' page download section for a copy of the form. https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/HowtoGetConnectedHETS270271.html

Questions	Answers
Who can use the HETS system?	The HIPAA Eligibility Transaction System (HETS) is intended to allow the release of eligibility data to Medicare Providers, Suppliers, or their authorized billing agents for the purpose of preparing an accurate Medicare claim, determining Beneficiary liability or determining eligibility for specific services. Such information may not be disclosed to anyone other than the Provider, Supplier, or Beneficiary for whom a claim is filed.
What are the hours and contact information for the HETS Help Desk?	The operational hours for the MCARE Help Desk are 7:00 AM - 7:00 PM ET Monday - Friday (with the exception of selected holidays). HETS submitters who contact the Help Desk outside of business hours have an opportunity to leave a voicemail for urgent issues. Messages are monitored 24 hours a day - depending on the severity of the issue, calls may be returned the next business day. Please contact the Help Desk if you have any questions. The Help Desk phone number is 1-866-324-7315. You can also email the help desk at mcare@cms.hhs.gov. This email address is monitored Monday - Friday 7AM - 7PM ET. Emails are typically answered within 24-48 business hours.
What is the minimum data required to do a search for eligibility?	The following information is required to run a search: Patient's Medicare Number (Health Insurance Claim Number [HICN], Medicare Beneficiary Identifier [MBI] or Railroad Retirement Board [RRB] Number), Patient's Full First Name, Patient's Full Last Name, and Patient's Date of Birth. HETS also supports alternate search options as outlined in Section 7.3 of the HETS 270/271 Companion Guide. Please refer to the Companion Guide for additional information: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html
I verified the patient's card and the information matches, why am I still not able to locate them in the system?	The HETS system obtains basic beneficiary information (name, date of birth, etc.) directly from the Social Security Administration (SSA) or Railroad Retirement Board (RRB) databases. The beneficiary may want to contact the SSA or RRB to verify that all their demographic information is correctly showing on their Medicare card.

Questions	Answers
Why does the 271 response not match what I receive from the IVR/DDE/other Medicare eligibility system?	Provider timely submittal of claims directly impacts the data returned on an eligibility inquiry. An eligibility response does not guarantee payment for a claim. As an eligibility requestor, you may see differences in Medicare eligibility responses based on the source provider (IVR, CWF inquiry, HETS 270/271) of your query due to the exchange of information between the sources. Typically these differences are due to a delay, up to 24 hours, in sharing information on nightly exchanges between the sources.
What is a HETS 270/271 Submitter ID number?	The HETS 270/271 Submitter ID number is the value that identifies your organization to the HETS 270/271 system. The HETS 270/271 Submitter ID is sent in every eligibility request.
Why does a beneficiary show active entitlement on other systems, but not on the HETS system?	Due to the logic used by the HETS 270/271 systems, if a beneficiary is deceased, deported, incarcerated, or of legal alien residency status in the United States, HETS will not return active entitlement. Some eligibility systems do not review this information before returning benefit information. Please refer to CMS HETS 270/271 5010 Companion Guide, Section 7.5: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html
What is a "Spell of Illness"?	A Medicare beneficiary is limited to a specific maximum number of days of covered inpatient hospital care, and covered post-hospital extended care in a SNF within a period of time known as a “spell of illness” or benefit period. Once these benefit days have been used, additional benefit days are not available until the spell of illness ends and a new benefit period begins. Please refer to CMS HETS 270/271 5010 Companion Guide, Section 7.8: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html
What is the availability of the HETS 270/271 Application?	The HETS 270/271 application is typically available 24 hours a day, 7 days a week. At this time, there are no standing HETS 270/271 maintenance windows. MCARE will notify HETS Trading Partners of any planned downtime. All current and archived downtime notifications are available on the cms.gov/HETSHelp website.
Where can I find the ASC X12N 005010X092A1 270/271 Implementation Guide/TR3?	CMS does not sponsor a copy of this guide. To obtain a copy of the 270/271 Implementation Guide/TR3 please contact Washington Publishing Company (WPC) at their website: http://store.x12.org/store/

Questions	Answers
Where can I find the HETS 270/271 Companion Guide?	The current version of the HETS 270/271 5010A1 Companion Guide is available for download on the HETSHelp website at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html
Where can I find an example of how to build the standard format of the TCP/IP Communication Transport Protocol Wrapper?	Refer to section 4.3.1 of the HETS 270/271 5010A1 Companion Guide for a detailed example: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html
I have received an error message but it is not an X12 format message, what should I do?	An error message occurs when the system detects an error that causes the system to not be able to read the ISA segment. When this situation occurs, a Proprietary error message will be returned. Please refer to Section 8.4 of the HETS 270/271 5010A1 Companion Guide for a list of all proprietary error messages and how to resolve them. https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html
How do I build the transaction for the HETS system?	Your organization will use the 5010 (ASC X12N 005010X092A1) 270/271 TR3, with reference to the HETS 270/271 Companion Guide to construct a transaction for the HETS 270/271 Application. You may access the 5010 HETS 270/271 Companion Guide at: https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html
When will a HETS 270/271 test system be made available to submitters so that upcoming HETS 270/271 system changes can be tested by HETS 270/271 submitters prior to actual implementation of changes?	At this time, CMS has no plans to offer a separate HETS 270/271 test system that would be available to HETS 270/271 submitters prior to production releases being implemented.
Will CMS require the 2100B NM103 segment in HETS 270 requests?	The 2100B NM103 element is required by the X12 5010A1 270/271 Implementation Guide/TR3 in all situations. In addition to the 2100B NM103 element, the following elements are also required to be present within the 2100B NM1 segment on all 5010A1 270 requests: NM101, NM102, NM108 and NM109.

Questions	Answers
Will HETS 270/271 validate the Medicare provider/supplier name within the NM103 element of the 5010A1 270 request or can a generic value like “PNAME” be sent in this field?	Per the X12 5010A1 TR3, the NM103 data element is a required field. Therefore, the HETS 270/271 application will verify that this field is not blank. Sending "PNAME" on a 5010A1 transaction would not result in a validation or a syntax error, but would be a violation of HIPAA's X12 standard intended use of that element. Thus, the sender of the transaction would be out of HIPAA compliance and at risk for future penalties and fines.
When submitting a query of the Submitter ID/NPI relationship using the HETS Desktop (HDT), what is the usual time before query results are displayed?	HDT displays online single query results within a few seconds. When using the HDT application's batch feature, it may take up to 24 hours to receive a results file. This processing time varies depending on the size of the inquiry file and overall GENTRAN system volume at the time of submission.
Please explain the data discrepancies between the Medicare eligibility responses returned by HETS 270/271 and the Medicare legacy eligibility systems like HIQA and HIQH that use the CWF database.	CMS has progressively worked to reduce the data discrepancies between responses returned by HETS 270/271 application and the Medicare legacy eligibility systems that utilize CWF. The HETS 270/271 Companion Guide is also a helpful resource regarding situations where HETS returns data differently than the CWF. https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html
When will HETS 270/271 be modified to return Psychiatric data in the 271 response to psychiatric providers?	HETS 270/271 currently returns Lifetime Psychiatric Limitation Data. See section 1.4 - Additional Information of the HETS 270/271 Companion Guide for the ROB. https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html
Does HETS 270/271 plan to add the patient status and patient indicator to the Home Health Prospective Payment System (PPS) episode information?	CMS has no plans to add this data at this time.

Questions	Answers
Will HETS 270/271 return the Hospice code for revocation reason, (e.g., transfer, death, or revoked)?	The Hospice Revocation Codes are returned in the HETS 271 responses. When Hospice care has been revoked (Hospice Revocation Code = 1, 2, or 3), then HETS 270/271 will return a Hospice termination date. If the final Hospice bill has not yet been received (Hospice Revocation Code = 0), then HETS 270/271 will not return a Hospice termination date. Refer to Section 7.16 of the HETS 270/271 Companion Guide for further explanation. https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Index.html
Does HETS 270/271 perform real-time validation of NPI numbers submitted in each 270 eligibility request?	HETS 270/271 validates submitted NPI numbers in real-time. If a submitter sends an ineligible NPI in a 270 request, HETS will reject the 270 request with a 271 response indicating that the NPI number is ineligible or not associated with the submitter's trading profile (which is managed via the HETS Desktop [HDT]).
If a HETS Desktop (HDT) User does not log in to EIDM/HDT every 60 days, does that render that User's organization list of Submitter ID/NPI relationships at risk for termination of the Submitter ID/NPI relationship in HPG?	No, the status of an individual's EIDM/HDT account has no bearing on the status of a Submitter ID/NPI relationship in HDT.
Is HETS 270/271 a real time or batch system?	HETS 270/271 is real-time processing system only. HETS submitters send a request and then wait for a response on the same connection. Submitters can re-use the same connection after the HETS response has been received (as long as the next request is sent immediately after the first response is received). HETS 270/271 does not support batch file processing.
Will the HETS 271 DSH response be modified to provide more than 27 months of historical eligibility data?	In 2018 CMS modified the HETS DSH response to allow historic searches of up to 48 months prior to the current date. At this time, CMS has no plans to modify the HETS DSH response to support any historic dates beyond 48 months.

Questions	Answers
How do I get a HETS 270/271 Submitter ID?	The MCARE Help Desk will provide you with your organization's Submitter ID number when you have established connectivity and are ready to test. If your organization has not received its Submitter ID number but has established a connection to HETS and is ready to test, contact the MCARE Help Desk to receive your Submitter ID number.
Why does the MCARE Help Desk ask for a HETS 270/271 Submitter ID when I call?	The Help Desk documents all telephone calls that are received. Your organization's Submitter ID number is used to cross-reference the record of all telephone calls from your organization.
What is Multi-Factor Authentication (MFA)?	MFA is an approach to security authentication that requires you to provide more than one form of a credential in order to prove your identity. CMS is requiring MFA service for CMS Enterprise Portal and HETS Desktop (HDT) Users. CMS uses Symantec's Validation and Identity Protection (VIP) service to add a layer of protection for your online identity. Symantec's VIP utilizes government-certified technology and techniques to provide this multi-factor authentication.
How do we use Multi-Factor Authentication?	CMS uses Multi-Factor Authentication (MFA) to grant access to the CMS Enterprise Portal and the HETS Desktop (HDT) application. Users will be required to enter their CMS Enterprise Portal User ID, Password, and a One Time Password (OTP) code. OTP is generated by a free Symantec application (VIP Access software) that can be downloaded to your desktop or smartphone, or alternatively, you can receive an OTP via a Short Message Service (SMS) voice phone call, or via E-mail once you have registered your device in the CMS Enterprise Portal. If you have registered an MFA token device, enter your User ID and Password, then select the registered MFA device from the drop down options. Once the code has been sent to the selected MFA device, Enter the code in the Security Code field and select login.
How do I get an MFA credential?	The CMS Enterprise Portal will prompt you to register an MFA credential when you request access to the HETS Desktop (HDT) application and have not already registered an MFA credential in the CMS Enterprise Portal. You will be given a choice of MFA token delivery methods. The primary MFA token delivery method is to download Symantec's Validation and Identity Protection (VIP) software and install it on your computer or a mobile device. Alternatively, if you require special support, you can set up Short Message Service (SMS) or Voice (IVR) services to deliver your MFA credential.

Questions	Answers
Where can I get the Multi-Factor Authentication (MFA) software?	You will need MFA software if you choose to receive your MFA credential on a computer or laptop or a mobile device. You will be required to download the MFA software from Symantec and install it on your device of choice. To download the desktop software for Windows or Mac, navigate to the Symantec VIP Center site at: https://idprotect.vip.symantec.com/desktop/home.v and follow the instructions. If using an iPhone, Android, Blackberry, or other mobile device, use your device to navigate to the Symantec VIP Center mobile site at: https://m.vip.symantec.com/home.v and follow the instructions. Text Message Short Message Services (SMS), E-mail One Time Password (OTP), and Interactive Voice Response (IVR) options do not require a software download.
I am being asked to type a Credential ID, where do I find the Credential ID?	The Credential ID is the 12-digit alphanumeric number on the top of the VIP Access software token that was downloaded to your device from Symantec. The Credential ID begins with four letters and ends with eight numbers.
How do I register additional devices to my user account?	You can register up to five MFA credentials in your user account. Additional MFA credentials can be added to your account after you have been prompted by the CMS Enterprise Portal to set up the first MFA credential. The “Register your Smartphone or Computer” hyperlink on the “My Profile” page will appear once you have successfully set up your first MFA credential. You can click on the link and add additional MFA devices to your user account. Please note that you cannot use the same phone number for the Short Message Service (SMS) and Voice (IVR) services – a single phone number can only be tied to one service at a time.
Will I be charged cell phone time each time I use Symantec VIP MFA on my mobile device?	It depends on what delivery method you use. The Symantec VIP MFA software is free. Once the Symantec VIP MFA application is downloaded and installed on the phone it does not utilize any cell time to generate the six-digit security code. Cell or network traffic is used to download the application to one’s mobile device. There are no recurring charges associated with the use of either software option. If you choose not to use the software option and select SMS or Voice OTP, carrier charges may apply.

Questions	Answers
How do I register for MFA if I receive an error when installing the software on my computer?	If you are having trouble downloading and installing the MFA software on your desktop or laptop, it is possibly due to your company's IT policy that disables users from installing any software on their company-provided machines. Check with your company's IT department for assistance. If your company does not allow you to install MFA software, one alternative is to use a mobile device that you control, or you can also use a voice call to obtain the One Time Password (OTP). You can refer to other instructions in the FAQ documents for information on cell phone installation and voice token usage.
Why can't I use the desktop MFA software or the mobile phone MFA software?	The CMS Enterprise Portal allows you to set up a Voice Response (IVR) or Short Message Service (SMS) delivery method for your One Time Password (OTP) that does not require an MFA software download. You can register a phone number and select SMS or Voice OTP, and then the CMS Enterprise Portal can register your phone number and delivery method with Symantec. After your MFA is activated, when you request access to the CMS Enterprise Portal you will receive either a phone call or text message that contains your OTP, depending on the delivery method that you select. The SMS and Voice OTP expire within thirty minutes of when they are sent, so please make sure you provide a phone number that will be accessible to you during your typical work hours. As an example, do not use a residential phone number if you will normally log in from your place of employment.
Can I access multiple Applications if I'm multi-factor authenticated?	Once you have been multi-factor authenticated in the CMS Enterprise Portal, if you do not log out of the system, you can access other protected CMS Applications that require MFA without having to be authenticated again with an MFA credential. If you log out of the system, when you log in again, you will be asked to present your MFA credential when accessing a protected CMS Application.

Questions	Answers
What is Remote Identity Proofing (RIDP)?	RIDP is the process of validating sufficient information about you (e.g., credit history, personal demographic information, and other indicators) to uniquely identify an individual. RIDP is a required service for most HETS Desktop (HDT) Users – existing HDT Users will not be required to complete the RIDP process. New HDT Users that have previously completed an RIDP process for the CMS Enterprise Portal will not need to complete the process again. CMS uses Experian to remotely perform identity proofing. You may have already encountered RIDP through various interactions with banking systems, credit reporting agencies, and shipping companies. The Experian identity verification service is used by CMS to confirm your identity when you need to access a protected CMS Application. When you log in to the CMS Enterprise Portal and request access to HETS Desktop (HDT), you will be prompted to RIDP if you have not been previously identity proofed to the level of assurance required by the CMS Enterprise Portal. You will be asked to provide a set of core credentials, which include: Full Name, Social Security Number, Date of Birth, Current Residential Address, and Personal Phone Number. The Experian identity verification service will use your core credentials to locate your personal information in Experian and generate a set of questions, referred to as out-of-wallet questions. Experian will attempt to verify your identity to the appropriate level of assurance with the information you provided. Most users are able to complete the ID proofing process in under five minutes. If you encounter problems with RIDP, you will be asked to contact Experian Support Services via phone to resolve any issues.

Questions	Answers
What happens to the data submitted for identity proofing?	The CMS Enterprise Portal collects your personal information, described as data that is unique to you as an individual, such as name, address, telephone number, Social Security Number, and date of birth. The CMS Enterprise Portal uses this personal information only to verify your identity. Your information will be sent to Experian, an external identity verification provider, to help us confirm your identity. If collected, we will validate your Social Security Number with Experian only for the purpose of verifying your identity. Experian verifies the information you give us against their records and may present you with questions based on your credit profile, called out-of-wallet questions. The out-of-wallet questions and answers, including financial history, are strictly between you and the Remote Identity Proofing (RIDP) service Experian; neither the CMS Enterprise Portal nor the HETS Desktop (HDT) application will store them. Experian is required by law to securely maintain this data for seven years. For more information regarding how CMS uses the information you provide, please read the CMS Privacy Act Statement at: http://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/Privacy/index.html
Will RIDP affect my credit?	No, this type of inquiry does not affect your credit score and you will not incur any charges related to this credit score inquiry. When you identity proof, Experian creates something called a soft inquiry. Soft inquiries are visible only to you, the consumer, and no one else. Soft inquiries have no impact on your credit report, history, or credit score other than being recorded and maintained for 23 months.
What happens if my identity cannot be verified during the online RIDP process?	If Experian cannot identity proof you online, you will be asked to contact either the Experian Verification Support Services Help Desk or the HETS Desktop (HDT) Help Desk, depending on the reason you failed RIDP. The system will provide you with a reference number to track your case. The Experian Help Desk cannot assist you if you do not have the reference number. If you are asked to contact the HDT Help Desk, you will be given a response code to help the HDT Help Desk perform the manual identity proofing process with you.
What happens if my identity cannot be verified during the Experian phone proofing RIDP process?	If you contact the Experian Verification Support Services Help Desk and your identity cannot be verified, you will be referred to the HETS Desktop (HDT) Help Desk to complete the manual identity proofing process.

Questions	Answers
How do I contact the HETS Desktop (HDT) Help Desk?	The HETS Desktop (HDT) Help Desk is open Monday through Friday from 7:00 a.m. to 7:00 p.m., Eastern Standard Time (EST). You can contact the HDT Help Desk using either of the following methods: Email address: mcare@cms.hhs.gov or Phone Number: 1-866-324-7315.
What are the Experian Help Desk hours of operation?	The Experian Help Desk is open Monday through Friday from 8:30 a.m. to 10:00 p.m., Saturday from 10:00 a.m. to 8:00 p.m., and Sunday from 11:00 a.m. to 8:00 p.m., EST.
What are some remote identity proofing tips for success?	The following items are some tips for remote identity proofing success: Name: You must use your full legal name. Refer to your Driver's License or financial account information. Your surname has to match the surname Experian has for you on file. Do not use nicknames. If you have a two-part name, enter the second part in the middle name field. (i.e., Billy Bob would have Billy in the first name field and Bob in the middle name field) Address: Enter your current residential address where you receive financial statements including credit cards and/or utilities • Address you most consistently use for billing purposes • Address associated with your credit report • If you have a recent change in address, you can try to ID proof with a prior address. • Do not enter any extraneous symbols in the address field. If you want to confirm the correct format, visit USPS Look Up a Zip Code at: https://tools.usps.com/go/ZipLookupAction!input.action Phone: Enter a personal landline phone number (if you have one). • A cell phone can be used, but a residential landline is preferred. Out-of-Wallet Questions: You will be asked a series of questions regarding your personal financial transactions/information. • Try to collect all of your information together before attempting the session. • Download a free copy of your credit report at http://www.annualcreditreport.com.

Questions	Answers
What are some remote identity proofing tips for success? (continued)	(continued from above) Consent: You will be asked to give consent to verify your identity information from your credit report. • The information is utilized only for purposes of identity proofing – "you are who you say you are." • The consent of utilizing the information does post as a soft inquiry on your credit report. The soft inquiry is visible only to you. • The consent/inquiry does not affect your credit score. Exclusions: If you have a Victim's Statement or a blocked or frozen file, you will NOT be able to complete the identity proofing process online. • After attempting online, you will be directed to call Experian's Consumer Services at 1-866-578-5409 to have the alert temporarily lifted so that you can attempt the ID proofing process. • If you are listed as deceased on the Social Security Administration's (SSA) Death Master File, you will not be able to complete the identity proofing process online. • You may contact the SSA at 1-800-269-0271. They will be able to make sure that your information is being reported correctly.
What is the maximum number of 270s I can send in a single batch file to HETS?	The HETS 270/271 application is real-time processing system only and does not accept eligibility batch files where there are multiple eligibility requests within each file. HETS 270/271 only accepts real-time 270 requests which contain one eligibility request per file.