Centers for Medicare & Medicaid Services

HETS Desktop (HDT)
User Guide

Version 2.0

9/4/2025

Table of Contents

List of Figures

List of Tables

1.1 Introduction

This HDT User Guide provides the information necessary for Clearinghouse and Direct Provider Submitters to effectively use the Health Insurance Portability and Accountability Act (HIPAA) Eligibility Transaction System (HETS) Desktop (HDT) application.

HDT leverages the Centers for Medicare and Medicaid Services (CMS) enterprise Identity Management (IDM) system for user access and verification.

1.1.1 HDT User Guide Intended Audience

The intended audience of the HDT User Guide consists of the following users:

- New HDT users who create their user accounts via IDM.
- Existing HDT users who created their user accounts via IDM or were migrated from the legacy Enterprise Identity Management system.

1.1.2 User Guide Purpose

Centers for Medicare & Medicaid Services (CMS) is dedicated to safeguarding Protected Health Information (PHI) and ensuring that only entitled Medicare Providers and Suppliers receive Medicare benefit information. CMS requires all Submitters to ensure that they are only sending active, valid Fee-for-Service (FFS) Medicare National Provider Identifier (NPI) numbers to the HETS 270/271 application.

Submitters must utilize the HDT application to register and maintain an updated record of their business relationships with their HETS 270/271 Provider and/or Supplier customers before submitting HETS 270/271 transactions. Additionally, Submitters can verify whether NPI numbers are eligible for use with the HETS 270/271 application.

This user guide is written to address specific actions in either the IDM Self-Service User Interface (UI) or the HDT application that are specific to HETS and HDT. This document does not replicate basic IDM functionality or processes that are outlined in available IDM user documents. Please see *Referenced Documents* for additional IDM information.

This user guide provides step-by-step instructions for performing the following tasks (based on access privileges) using the IDM Self-Service UI:

- How to request HDT access via IDM

This user guide also provides step-by-step instructions for performing the following tasks using the HDT application (when applicable):

- NPI management via the HDT UI, including querying, adding, or terminating Submitter ID/NPI relationships
- Downloading a list of active NPI/Submitter attestations associated with your organization, which are created by Medicare Providers or Suppliers
- NPI management via the HDT NPI Batch Management, including querying, adding, or terminating Submitter ID/NPI relationships
- Troubleshooting common HDT errors

1.1.3 Identity Management (IDM) System Overview

CMS created the IDM system to provide business partners with a means to request and obtain a single User ID, which they can use to access one or more CMS applications, including HDT. The IDM system employs a cloud-based, distributed architecture that meets the needs of CMS applications while delivering enhanced user experience on desktop and laptop computers, as well as tablet and smartphone mobile devices.

The IDM security policy includes processes to disable inactive IDM user accounts that are inactive for sixty days. These users are required to update their IDM password during the reactivation process. IDM users who remain inactive for two years will have their accounts removed. These users are notified via email before their account is removed. IDM accounts that have been removed cannot be reinstated. Users who are removed need to create a new IDM account, complete Remote Identity Proofing (RIDP), and request any application-specific access, like HDT, via IDM. Additional information about IDM is available in *Referenced Documents*.

1.1.4 HDT Application Overview

Users access the HDT application after authenticating their identity using an IDM User ID and password. Approved IDM users must add the HDT role to their IDM profile via the IDM UI, then obtain CMS approval before HDT access will be granted.

Submitters use the HDT application to:

- Register their HETS 270/271 Provider/Supplier customers with CMS to establish an NPI/Submitter relationship
- Maintain a list of all NPIs that their organization will be sending to the HETS 270/271 application
- View a list of associated NPIs and their HETS trading status
- Query the status for one or more NPIs via NPI management
- Clearinghouse Submitters can download a list of all active Medicare Provider/Providers and Suppliers who created attestations

The HDT application validates NPIs that are either being queried or added by the Submitter to ensure that they are valid FFS Medicare Providers or Suppliers. Additionally, HDT will check the status of an NPI with Medicare daily. If an NPI is deemed to be invalid by Medicare, the NPI will also be invalid in HDT and will be prohibited from receiving PHI from the HETS 270/271 application.

In addition to validating that the NPIs submitted to the HETS 270/271 application are active and valid with Medicare, the HDT application will validate that there is a known Submitter/Provider relationship between the HETS 270/271 Submitter and the FFS Medicare Provider or Supplier.

The HDT application allows for both manual and batch NPI management processes. The manual NPI management options allow Clearinghouse and Direct Provider Submitters to query, add, and terminate their relationships with Providers and/or Suppliers one NPI at a time. The screen displays the session’s most current 25 responses in order, with the most recent response listed first.

The batch NPI management option allows Clearinghouse Submitters to query, add, and terminate their relationships for multiple NPIs at one time. The NPIs must be submitted in a flat text file that can be uploaded via the HDT application. HDT Clearinghouse Submitter Users can upload batch files and then receive response files back via the HDT application. HDT batch input files are stored in the user’s HDT history for 60 days before they are archived; HDT batch output files are stored in the user’s HDT history for at least 120 days before they are archived.

The HDT application is integrated with the HETS 270/271 application. The NPIs submitted on 270 eligibility requests will be validated in real-time. If a Submitter sends an eligibility request with an NPI number that is a) not on file with CMS, b) not an active, valid FFS Medicare Provider at the time the request is processed, or c) not found as associated with the Submitter, then a 271 AAA error (with an appropriate error code) will be returned instead of entitlement information. Refer to Section 8.3 of the HETS 270/271 Companion Guide for more information on the 271 AAA error codes.

In the future, the HETS 270/271 application will transition from real-time validation of NPI/Submitter relationships (created by the Submitter via HDT) to NPI/Submitter attestations (created by the Medicare Provider/Supplier).

- HETS Clearinghouse Submitters must collaborate with their Medicare Provider/Supplier customers to ensure that NPI attestations are recorded and maintained via the URLs per MAC jurisdiction provided on this page.
- HETS Direct Provider/ Supplier Submitters will not create attestations for their NPIs; they will contact MCARE when an NPI needs to be added in the future.
- Medicare Provider/ Supplier NPIs that do not use HETS or are only sent to HETS by non-Clearinghouse Submitters do not need to create attestations.

1.2 Referenced Documents

IDM maintains a current *CMS IDM User Guide* (and other helpful documentation) on the CMS IDM User Guides & Documentation page. Please refer to that page for information about IDM registration, multi-factor authentication for IDM accounts, and basic IDM account maintenance tasks.

IDM also maintains several valid documents related to Remote Identity Proofing (RIDP). All HDT users must complete RIDP.

The *HETS 270/271 Companion Guide* provides information related to the HETS 270/271 application described throughout this document. Users can obtain the latest version of the *HETS 270/271 Companion Guide* via this link.

If problems or questions arise while accessing the HDT application, contact the MCARE Help Desk at 1-866-324-7315 or MCARE@cms.hhs.gov, Monday through Friday, from 7:00 am to 7:00 pm ET.

1.3 Quick Reference Guide

Table 1: Quick Reference Guide

Questions	Answers
Need to sign in to HDT?	Navigate to https://HDT.hetsp-haa.cms.gov/HDT/ or see Section Log In to the HDT Application
Need to sign in to IDM?	Navigate to https://home.idm.cms.gov/ or refer to Section 5 of the CMS IDM User Guide
Need to create an entirely new IDM account?	Refer to Section 4 of the CMS IDM User Guide

Questions	Answers
Need to add a Multi-factor Authentication (MFA) device to your IDM account?	Refer to Section 11 of the CMS IDM User Guide
Has your IDM password been reset?	Refer to Section 10 of the CMS IDM User Guide
Locked out of IDM?	Refer to Section 10 of the CMS IDM User Guide
Need to change your IDM password?	Refer to Section 10 of the CMS IDM User Guide
Need to add an HDT role to an existing account?	See Section *How to Request HDT Access Via IDM*
Need to manage your roles in IDM?	Refer to Sections 6-10 of the CMS IDM User Guide
Need help with Remote Identity Proofing?	Refer to IDM's RIDP resources
Need to create a new NPI relationship?	See Section *NPI Management*
Need to submit an HDT Batch file?	See Section *NPI Batch Management*
Need to download a list of your customers' active attestations?	See Section *Download Active Provider Attestation List*
Getting an error in HDT?	See Section *HDT Error Messages*

1.4 Prepare to Access the HDT Application via IDM

Users who access HDT using IDM with a desktop or laptop computer may need to perform software updates or configure web browser settings and privacy settings. Users who access HDT using IDM via a mobile computing device such as a smartphone or tablet have less control over updates and privacy settings. Therefore, the procedures discussed in this section may not apply to mobile device users.

1.4.1 Verify Web Browser Support

The HDT application and IDM were tested for compatibility with current versions of the following modern web browsers:

- Microsoft Edge (Legacy) [1]
- Google Chrome
- Mozilla Firefox
- Safari

All the web browsers listed above are configured by default to receive regular security updates and patches. Even in cases where the user's organization manages operating system and application software updates, users who access HDT via IDM with one of these web browsers should not encounter compatibility issues.

1.4.2 Verify Screen Resolution

The HDT application and IDM are optimally viewed on a display resolution of 1366 x 768. All images displayed on modern computing devices are composed of a matrix of thousands of tiny

[1] Microsoft Edge (Legacy) is the default web browser on modern Windows PCs. Many enterprise users still have this as their default web browser.

dots, called pixels. This matrix is expressed as width times height (for example, 1366 pixels wide x 768 pixels high, or 1366 x 768).

A device's screen resolution, therefore, refers to the size of this matrix. The more pixels the screen can display, the higher the resolution, and the better on-screen text and images will look. The default display resolution setting for modern desktop, laptop, and mobile computing devices generally equals or exceeds 1366 x 768. The HDT application and IDM support older devices with a minimum resolution of 800 x 600.

Note: Modern desktop and laptop computers typically configure their operating systems to display resolutions that meet or exceed 1366 x 768 pixels. Users of older devices or operating systems may need to change their display resolution settings if the current setting does not display the IDM system correctly.

1.4.3 Cautions and Warnings

Web browser capabilities such as back, forward, refresh, and logging out should not be used during HDT application sessions.

Users should manually enter all internet addresses (Uniform Resource Locators, or URLs) into the internet browsers. CMS discourages users from utilizing browser bookmarks with the HDT application.

To optimize access to the HDT application, please disable your pop-up blocker before use.

CMS discourages HDT users from using the autofill or auto-populate features of internet browsers. Users should disable these features in their browsers when using HDT.

HDT users should adjust their internet browser settings to prevent caching when using HDT. Web browsers with large cache settings can store web pages on the user's computer for extended periods. Because the HDT application framework has been developed to utilize similar page components, the user's browser must be configured to ensure that it attempts to locate and retrieve a fresh instance of the HDT page and its data content.

HDT users should enable JavaScript and adjust any zoom features to ensure that they are not seeing the screen in too broad a view.

HDT users should disable Compatibility View settings in their web browsers to ensure the proper display of HDT pages.

HDT dynamically optimizes layout and content based on screen display size. Users with a limited display size may see some display items consolidated into menus or icons, like *Figure 1: Menu Icon* in the upper left corner of the screen.

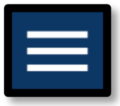


Figure 1: Menu Icon

If the user switches to a larger display, some previously consolidated display items may expand into selectable elements on the page, rather than being consolidated into menus. CMS recommends that HDT users optimize their displays to the maximum readable size.

1.5 Description of Key HDT User Authentication Mechanisms

The HDT application uses IDM to confirm the user’s account credentials. In addition to standard IDM security mechanisms, HDT uses the following security mechanisms:

- HDT User ID policy
- HDT password policy

1.5.1 HDT User ID Policy

The HDT User ID policy combines application-specific guidelines and CMS password policy. IDM User IDs that are used to access HDT must conform to the following guidelines:

- Only personnel from HETS Clearinghouse and Direct Provider Submitters will be granted permission to access the HDT application. Users must be associated with an organization that has an active, valid HETS 270/271 Submitter ID.
- HDT users must have an IDM User ID that has 32 characters or fewer to utilize the HDT application.
- The HDT application allows the IDM User ID and the IDM user's first and last names to contain certain special characters. Special characters apostrophe (‘ ‘ ‘), hyphen (‘ - ’), and spaces are compatible with HDT in the User ID and first and/or last name. Period (‘ . ‘) and underscore (‘ _ ‘) are also permitted in the User ID. The at sign (‘ @ ‘) is allowed as part of the User ID, but only when used as part of an email address format.

Users who request the HDT role for an existing IDM User ID that is greater than 32 characters and/or have a User ID or user first or last name that contains any special characters outside of the allowable situations noted above will not be granted access to the HDT application.

1.5.2 HDT Password Policy

The HDT password policy combines application-specific guidelines and the CMS password policy. Passwords that are used to access HDT must conform to the following guidelines:

- They must be at least 15 characters in length.
- They must contain one uppercase letter, one lowercase letter, and one number.
- Special characters are optional for use in the password. If used, the following special characters are acceptable: “ ! # $ % & ‘ ( ) * + , - . / \ : ; < = > ? @ [ ] ^ _ ` { | } ~.
- They must NOT contain a space.
- They must NOT contain parts of the user’s First Name, Last Name, or User ID.

1.6 How to Request HDT Access Via IDM

New HDT users can request access to the application (and an appropriate role) by using the ***Role Request*** button located on the IDM’s Self-Service UI or the Role Request taskbar option.

Note: The Role Request function is used to request access to HDT when the user does not currently have access.

HDT role requests consist of the following steps:

1. The user signs into their existing IDM account.
2. The user selects ‘Role Request’ in the IDM Self-Service UI.
3. The user selects the HDT application from the list of various IDM-based applications.
4. The user selects an appropriate HDT role.
5. The user provides a justification reason.
6. The user reviews and submits the request.

If needed, the user completes the Remote Identity Proofing (RIDP) process. [2]

1.6.1 How to Request Access and Role to the HDT Application

This section provides the steps that users must follow to request HDT access with the appropriate role.

1. Select the ***Role Request*** button located on the IDM Self-Service UI or select the Role Request taskbar option. Role Request UI appears. [3, 4]

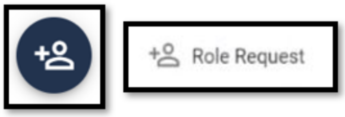


Figure 2: Role Request Button and Role Request Taskbar Option

2. Use the Select Application drop-down menu to select an application. [5]
3. Enter “HDT” and you will have an option to select the HDT application. [6]

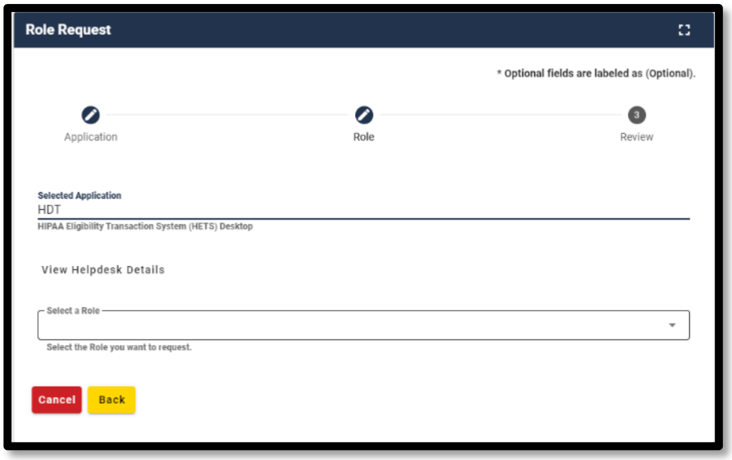
[2] RIDP is explained in the Remote Identity Proofing section.

[3] The Role Request UI provides prompts and screen tips that guide the user through each step to assist users with entering information in the proper syntax and/or format.

[4] The prompts for conditional information, such as RIDP, depend on the role that is being requested; hence, they may not appear until a role is selected.

[5] The Select Application dropdown menu will display all applications unless the user already has a role in that application.

[6] The Select Application drop-down menu will display all applications unless the user already has a role in that application.



Role Request

* Optional fields are labeled as (Optional).

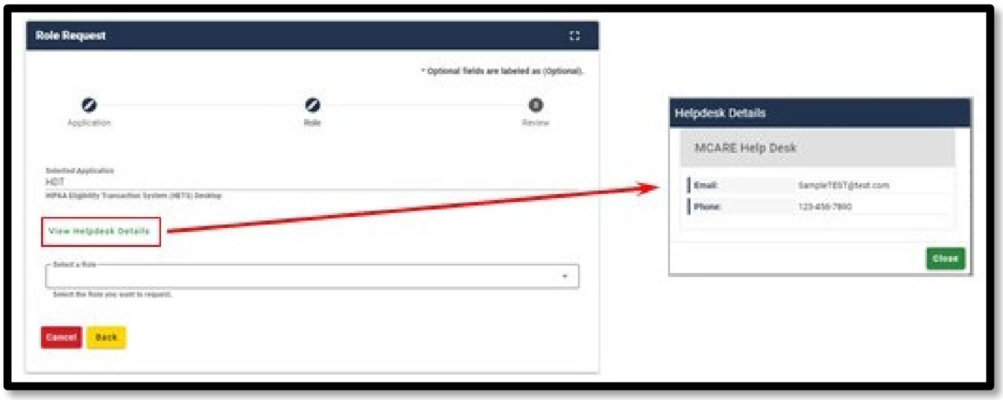
Selected Application
HDT
HIPAA Eligibility Transaction System (HETS) Desktop

Select a Role

Select the Role you want to request.

Figure 3: Role Request that Requires Application and Role

4. (Optional) Select the ***View Helpdesk Details*** button to display the Application Helpdesk Details UI. [7]



Role Request

* Optional fields are labeled as (Optional).

Selected Application
HDT
HIPAA Eligibility Transaction System (HETS) Desktop

Select a Role

Select the Role you want to request.

Helpdesk Details

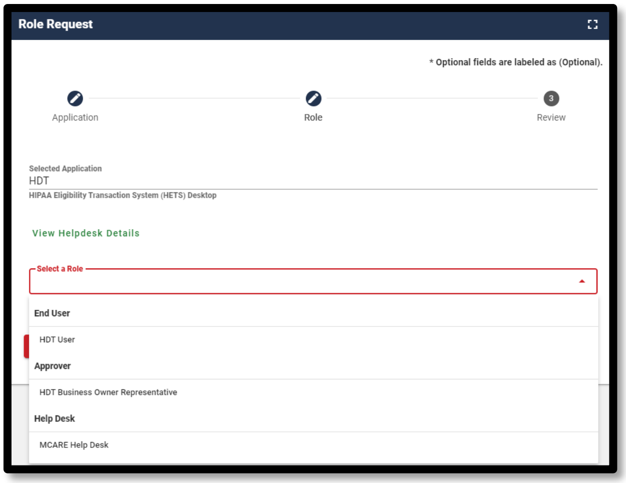
MCARE Help Desk

Email:	SampleTEST@test.com
Phone:	123-456-7890

Figure 4: Role Request Helpdesk Details (Optional Step)

5. Use the Role drop-down menu to select a Role. The majority of HDT users should choose the “End User” or “HDT User” role.

[7] The MCARE Helpdesk may need to be contacted if there are problems with the role request. Select the Close button to hide the Helpdesk Details window.



* Optional fields are labeled as (Optional).

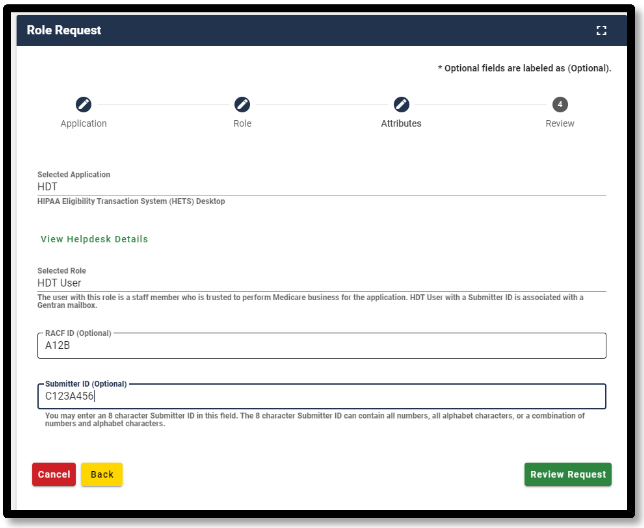
Selected Application
HDT
HIPAA Eligibility Transaction System (HETS) Desktop

Select a Role

End User
HDT User
Approver
HDT Business Owner Representative
Help Desk
MCARE Help Desk

Figure 5: Role Request Specifying HDT Role

6. Enter the user's CMS RACF ID (if applicable) and HETS 270/271 Submitter ID information as necessary, as shown in *Figure 6: Role Request Specifying Additional Details*.



* Optional fields are labeled as (Optional).

Selected Application
HDT
HIPAA Eligibility Transaction System (HETS) Desktop

Selected Role
HDT User
The user with this role is a staff member who is trusted to perform Medicare business for the application. HDT User with a Submitter ID is associated with a Gentran mailbox.

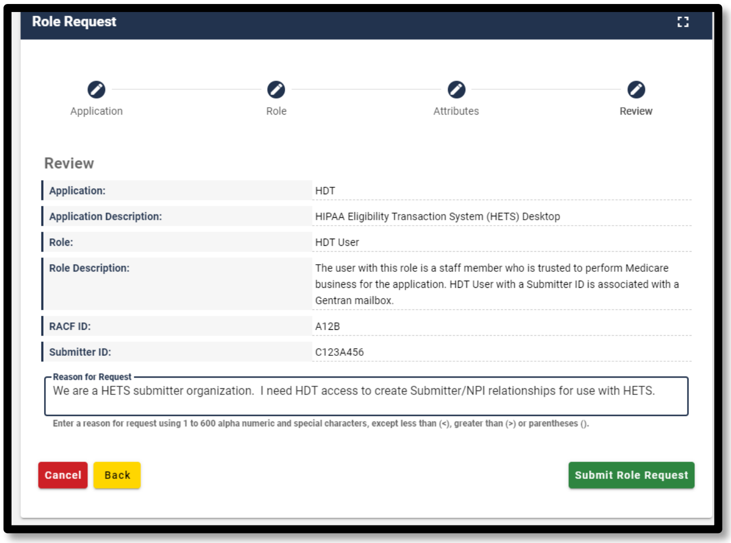
RACF ID (Optional)
A12B

Submitter ID (Optional)
C123A456

You may enter an 8 character Submitter ID in this field. The 8 character Submitter ID can contain all numbers, all alphabet characters, or a combination of numbers and alphabet characters.

Figure 6: Role Request Specifying Additional Details

7. Select the ***Review Request*** button.
8. The screen will update to include a freeform text box titled "Reason for Request." Enter a brief justification statement into this field to justify the role request.



Review

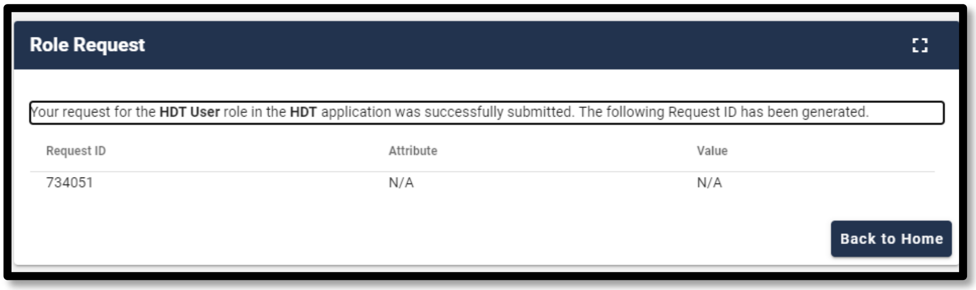
Application:	HDT
Application Description:	HIPAA Eligibility Transaction System (HETS) Desktop
Role:	HDT User
Role Description:	The user with this role is a staff member who is trusted to perform Medicare business for the application. HDT User with a Submitter ID is associated with a Gentran mailbox.
RACF ID:	A12B
Submitter ID:	C123A456

Reason for Request: We are a HETS submitter organization. I need HDT access to create Submitter/NPI relationships for use with HETS.

Enter a reason for request using 1 to 600 alpha numeric and special characters, except less than (<), greater than (>) or parentheses ().

Figure 7: Role Request Ready for Submission

9. Select the ***Submit Role Request*** button. [8], [9]



Your request for the **HDT User** role in the **HDT** application was successfully submitted. The following Request ID has been generated.

Request ID	Attribute	Value
734051	N/A	N/A

Figure 8: Successful Role Request Message

10. The Role Request UI displays a Request ID and a message that informs the user that the request was successfully submitted. [10]
11. The My Requests indicator on the Self-Service UI increments to display the user's current number of pending requests.

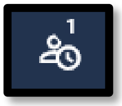


Figure 9: My Requests Indicator

12. Select the ***Back to Home*** button to return to the Self-Service UI.

[8] The role request is forwarded to the user's approver of record. Note that some applications may require approval from multiple approvers.

[9] Select the Back button to remain in the Role Request form and make changes or select the Cancel link to terminate the Role request process and reset the Role Request form.

[10] An email is sent to the user's email address of record, which indicates that the role request was successfully submitted.

In addition to sending the user an email that indicates the user’s request was submitted, the IDM system also sends the user subsequent emails related to the status of each request as follows:

- **Approve**: The system sends an email to the user’s address on record, which indicates that the request was approved. It also indicates where users can obtain assistance if they have questions.
- **Reject**: The system sends an email to the user’s address on record, which indicates that the request was rejected. It also indicates where users can obtain assistance if they have questions.
- **Expire**: The system sends an email to the user’s address on record, which indicates that the request expired due to no action taken by an approver. It also indicates where the user can obtain assistance if they have questions.

1.7 Using the HDT Application

The following sub-sections provide detailed, step-by-step instructions on how to use the various features of the HDT application.

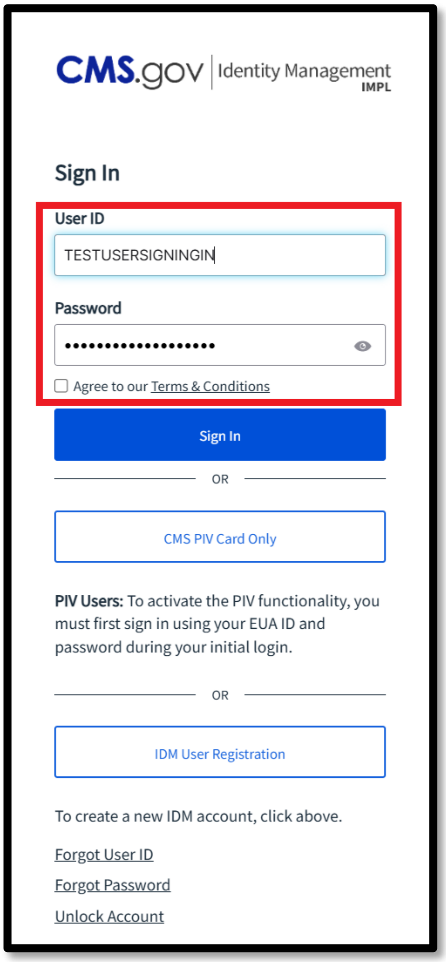
1.7.1 Log In to the HDT Application

HDT utilizes the IDM system to authenticate each user and grants that user access to the application. This section provides the steps that users must follow to sign in to HDT via the CMS IDM system.

1. Enter the CMS Applications Portal URL in a web browser:

   https://HDT.hetsp-haa.cms.gov/HDT/

   Please do not bookmark this or any other page in your internet browser. CMS discourages users from utilizing browser bookmarks with the HDT application. The CMS IDM system screen displays as illustrated in *Figure 10: IDM System Sign In Window***.**



User ID

TESTUSERSIGNINGIN

Password

••••••••••••••••••

□ Agree to our Terms & Conditions

PIV Users: To activate the PIV functionality, you must first sign in using your EUA ID and password during your initial login.

To create a new IDM account, click above.

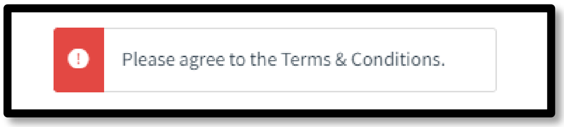
Forgot User ID

Forgot Password

Unlock Account

Figure 10: IDM System Sign In Window

2. Type the User ID into the User ID field.
3. Type the Password into the Password field.
4. Select the check box to acknowledge agreement with the Terms & Conditions. Failure to select the check box will result in an error, as illustrated in *Figure 11: An Example Sign in Error: Agree to Terms & Conditions.*

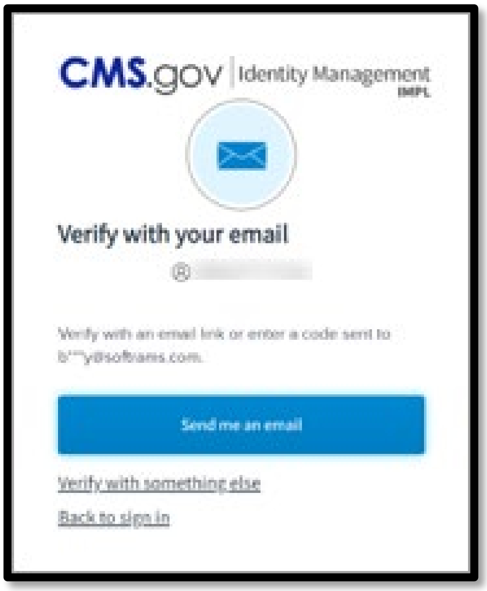


Please agree to the Terms & Conditions.

Figure 11: An Example Sign in Error: Agree to Terms & Conditions

5. Select the ***Sign In*** button. The MFA One-time Password (OTP) Request window appears.

Note: The IDM system uses Email MFA by default, so the steps provided in this procedure follow that default. Users with alternative MFA devices should use the appropriate method for that MFA device.



Verify with your email

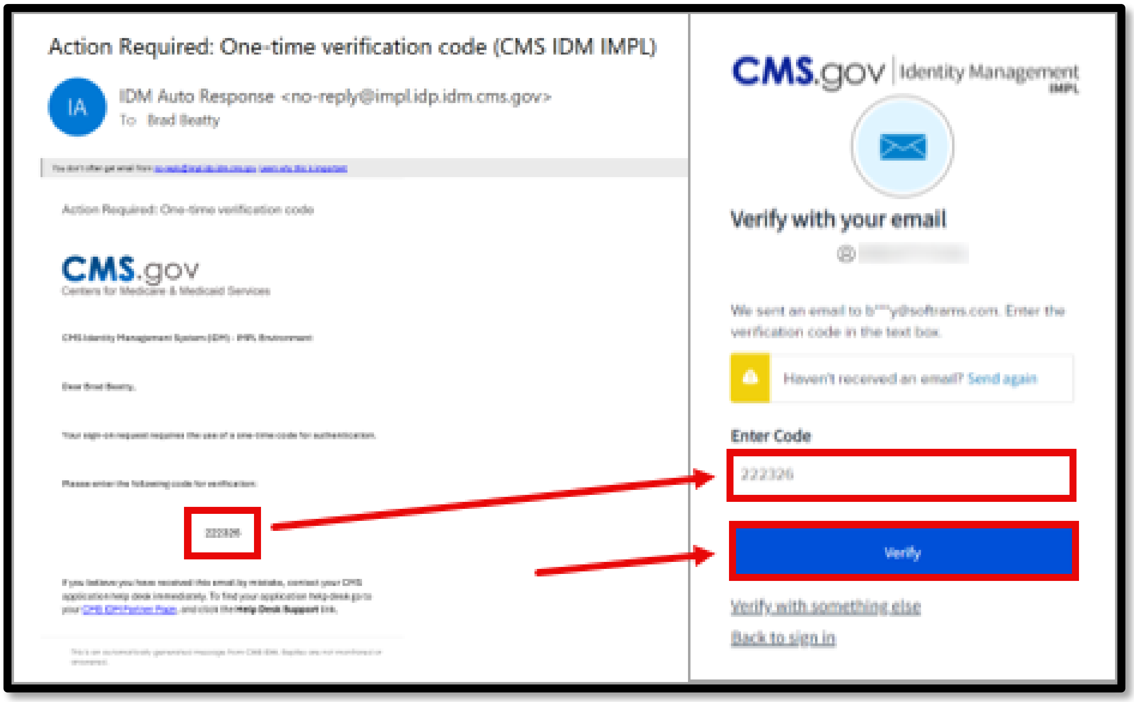
[redacted]

Verify with an email link or enter a code sent to b***y@softrams.com.

Figure 12: MFA OTP Request Window

6. Select the ***Send me the code*** button to request an OTP when the Verify with your email Authentication UI appears.

   The IDM system also allows the use of other MFA devices. The OTP delivery method can be an email, a voice message, a text message, or a push notification, depending on the user’s MFA device choice.



Action Required: One-time verification code (CMS IDM IMPL)

IDM Auto Response <no-reply@impl.idp.idm.cms.gov>
To Brad Beatty

You don't often get email from no-reply@impl.idp.idm.cms.gov. Learn why this is important

Action Required: One-time verification code

CMS.gov
Centers for Medicare & Medicaid Services

CMS Identity Management System (IDM) - IMPL Environment

Dear Brad Beatty,

Your sign-on request requires the use of a one-time code for authentication.

Please enter the following code for verification:

222326

If you believe you have received this email by mistake, contact your CMS application help desk immediately. To find your application help desk go to your CMS IDM Partner Page, and click the Help Desk Support link.

This is an automatically generated message from CMS IDM. Replies are not monitored or answered.

CMS.gov | Identity Management IMPL

Verify with your email

@ [redacted]

We sent an email to b***y@softrams.com. Enter the verification code in the text box.

Haven't received an email? Send again

Enter Code

222326

Figure 13: Sample MFA OTP Email and the MFA Verification Window

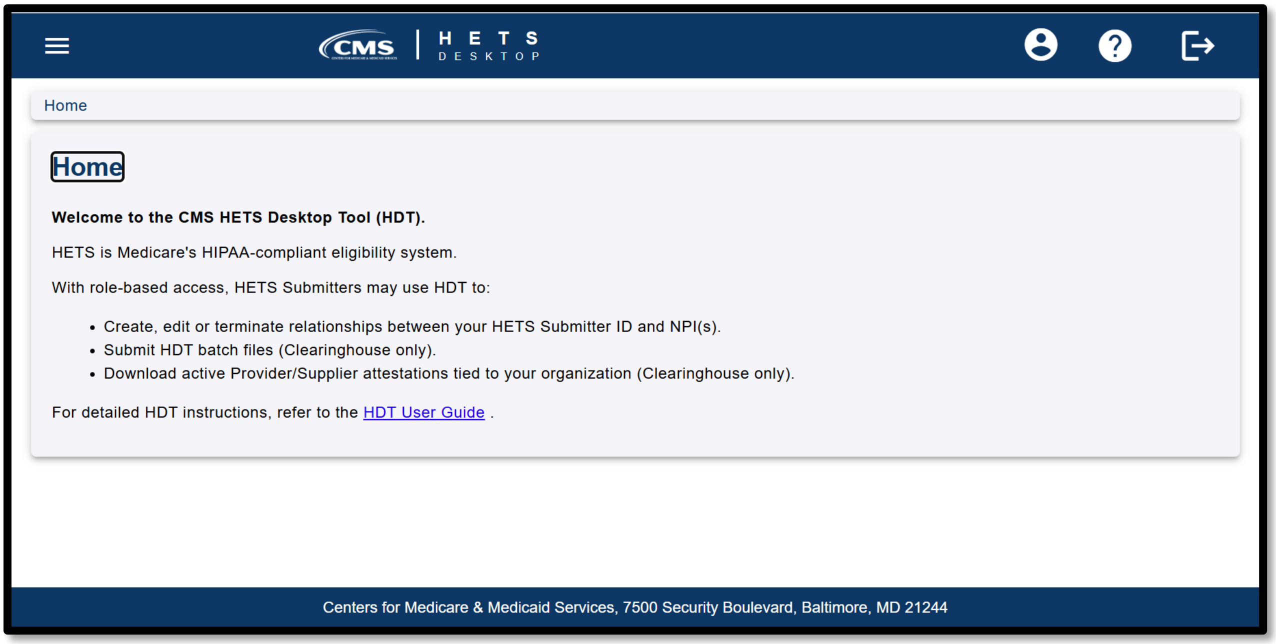
7. The MFA device returns an OTP. Enter the OTP into the 'Enter Code' field. If the MFA device uses push notifications, a code is not required.

Note:

- The user must enter the OTP within approximately 30 seconds of completing Step 6, or the Sign In window displays a message that asks, “Haven’t received an email? Send again.” as illustrated by *Figure 13: Sample MFA OTP Email and the MFA Verification Window.*
- The user may select the ***Send again*** link to request another OTP if the original OTP request failed.

8. Select the ***Verify*** button. Possible system responses include:
    - **Successful Sign In**: The user is taken to the HETS Desktop home page, as illustrated by *Figure 14: HETS Desktop Home Screen.*
    - **Unsuccessful Sign In**: Take corrective action based on the error message that displays. Additionally, verify the accuracy of the user ID and password and attempt to sign in again.

HETS Desktop Home Screen



Home

Home

Welcome to the CMS HETS Desktop Tool (HDT).

HETS is Medicare's HIPAA-compliant eligibility system.

With role-based access, HETS Submitters may use HDT to:

- Create, edit or terminate relationships between your HETS Submitter ID and NPI(s).
- Submit HDT batch files (Clearinghouse only).
- Download active Provider/Supplier attestations tied to your organization (Clearinghouse only).

For detailed HDT instructions, refer to the HDT User Guide .

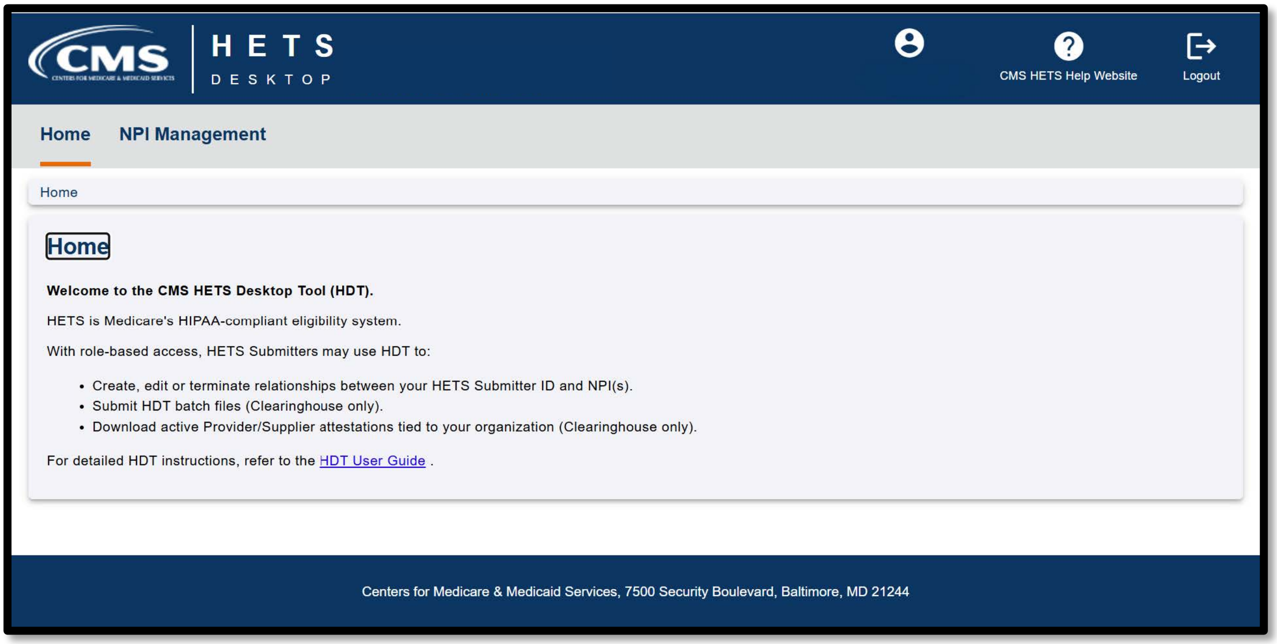
Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 14: HETS Desktop Home Screen

When users log in to the HDT application, the HETS Desktop home screen displays as illustrated in *Figure 14: HETS Desktop Home Screen***.**

Note: HDT dynamically optimizes layout and content based on screen display size. Users with a limited display size may see some display items consolidated into a single menu. Icons may also appear without titles in the limited display layout. If a user updates to larger display settings, some items that were previously consolidated into menus may expand to selectable items on the page instead. Similarly, some icons may now contain titles.

CMS recommends that HDT users optimize their displays to the maximum readable size. *Figure 14: HETS Desktop Home Screen* illustrates the HETS Desktop Home Screen page with a limited display size (and some display items consolidated into the menu at the upper left corner. The following image, *Figure 15: HETS Desktop Home Screen Expanded View*, illustrates the same HETS Desktop Home Screen page displayed on a larger screen (with the menu removed).



Home

Welcome to the CMS HETS Desktop Tool (HDT).

HETS is Medicare's HIPAA-compliant eligibility system.

With role-based access, HETS Submitters may use HDT to:

- Create, edit or terminate relationships between your HETS Submitter ID and NPI(s).
- Submit HDT batch files (Clearinghouse only).
- Download active Provider/Supplier attestations tied to your organization (Clearinghouse only).

For detailed HDT instructions, refer to the HDT User Guide .

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 15: HETS Desktop Home Screen Expanded View

Depending upon your HDT role, your navigation options (using menus, tabs, and/or icons) may include:

- **Home**: The HDT User Interface home page.
- **NPI Management:** Selecting NPI Management shows two sub-options for most users:
  - **NPI Management List:** This option is available to Clearinghouse and Direct Provider Submitters. Allows HETS Submitters to add relationships, terminate relationships, and/or query NPI numbers one at a time. As a new feature, the NPI Management section also allows Clearinghouse Submitters to view the Provider Attestation Status between a Medicare Provider or Supplier and their organization's unique ID (if any attestation exists).
  - **NPI Batch Management:** This option is available to Clearinghouse Submitters only. Clearinghouse Submitters can access the NPI Batch Management tool to upload batch files and create, terminate, or inquire about the status of Submitter ID/NPI relationships that are on file.
- **CMS HETSHelp Website**: Provides links to the CMS HETSHelp Website.
- **Logout**: Closes the active HDT application session and redirects the User to the CMS IDM System Sign In page, as illustrated in *Figure 24: IDM System Sign In Page*.

1.7.2 Application Layout

The application layout in the Site Map, as illustrated in *Figure 23: HDT Application Site Map*, is outlined as follows:

The links to navigate through the HDT application are:

- Home

- NPI Management
- NPI Management (data entry screen)
- NPI Batch Management (available for Clearinghouse Submitters only)

The icons available for selection through the HDT application include:

- Menu (depending on screen display, this may appear as an icon or instead as separate tabs for different tasks.

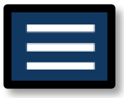


Figure 16: Menu Icon

- User Information (depending on screen display, may include the IDM User ID and the IDM User's name)

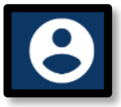


Figure 17: User Information Icon

- CMS HETS Help Website (depending on screen display, may include a title identifying that this is an external link to the CMS HETSHelp Website)

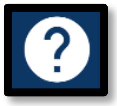


Figure 18: CMS HETS Help Website Icon

- View (the word 'View' will appear when hovering over this icon)

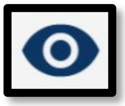


Figure 19: View Icon

- Terminate (the word 'Terminate' will appear when hovering over this icon)

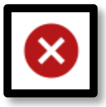


Figure 20: Terminate Icon

- Download File (the phrase 'Download File' will appear when hovering over this icon

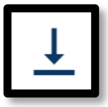


Figure 21: Download File Icon

- Logout (depending on screen display, may include the title 'Logout')

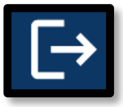
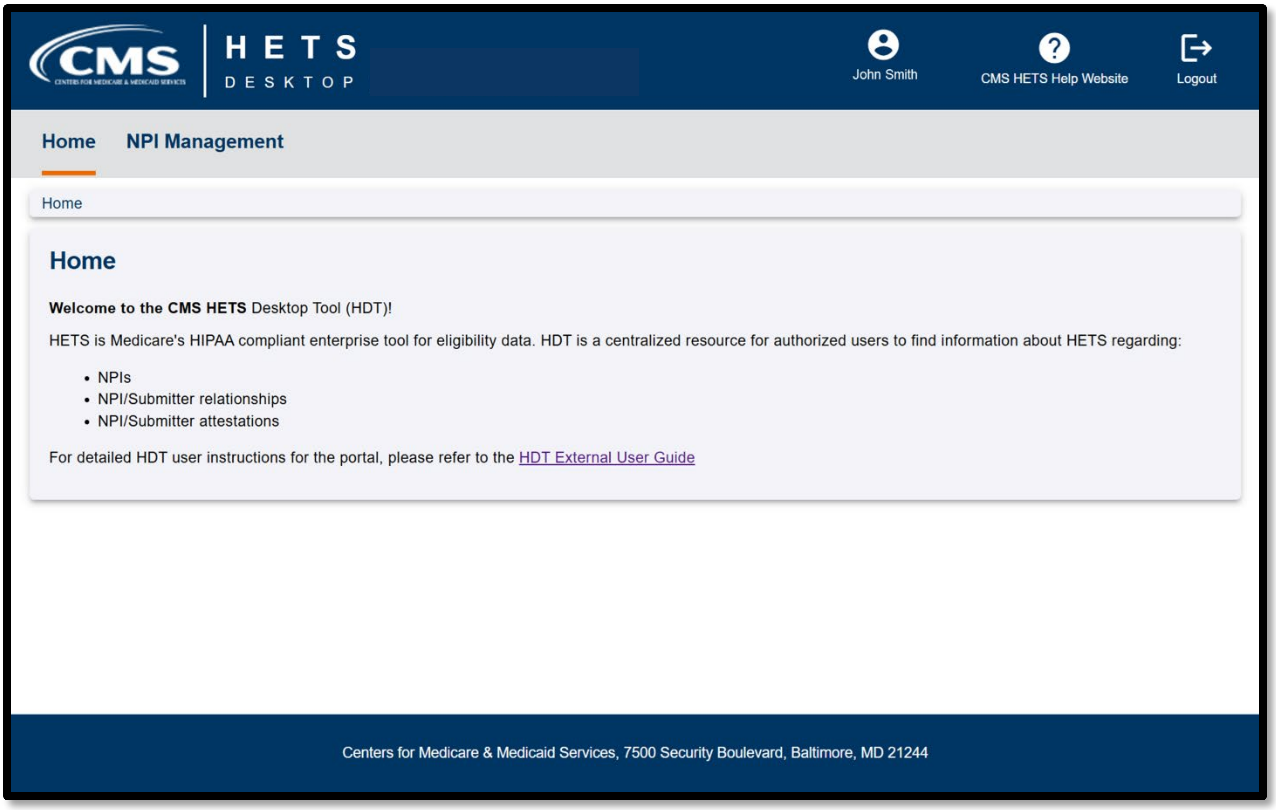


Figure 22: Logout Icon



Home

Welcome to the CMS HETS Desktop Tool (HDT)!

HETS is Medicare's HIPAA compliant enterprise tool for eligibility data. HDT is a centralized resource for authorized users to find information about HETS regarding:

- NPIs
- NPI/Submitter relationships
- NPI/Submitter attestations

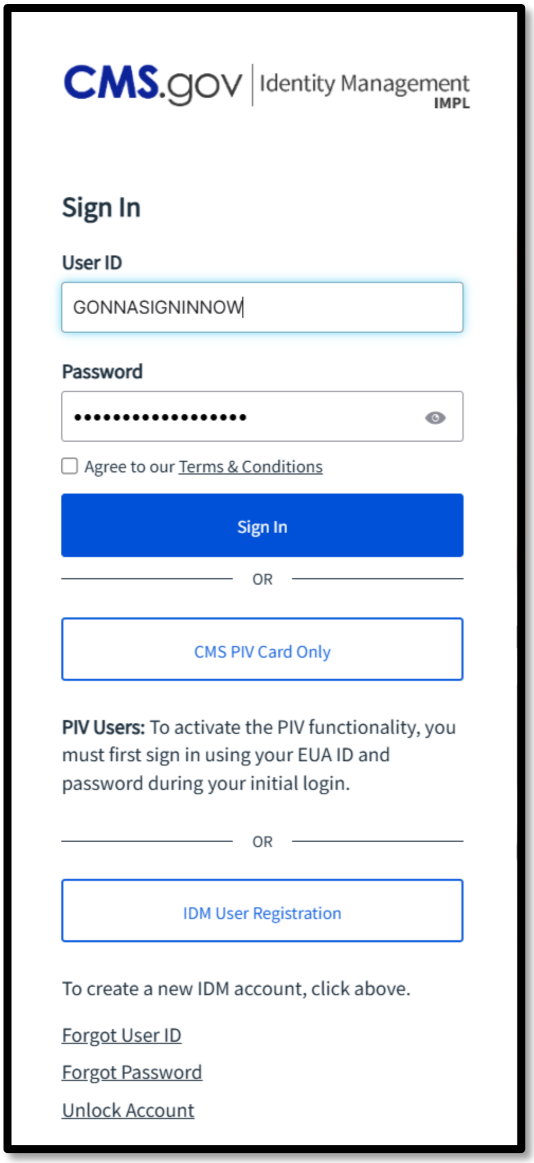
For detailed HDT user instructions for the portal, please refer to the HDT External User Guide

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 23: HDT Application Site Map

1.7.3 Exiting the Application

Select the ***Logout*** icon in the upper right corner of any screen in the HDT Application to log out of the HDT application. You will be logged out of the HDT application and returned to the IDM System Sign In page, as illustrated by *Figure 24: IDM System Sign In* **.**



CMS.gov | Identity Management IMPL

Sign In

User ID

GONNASIGNINNOW

Password

••••••••••••••••••

□ Agree to our Terms & Conditions

PIV Users: To activate the PIV functionality, you must first sign in using your EUA ID and password during your initial login.

To create a new IDM account, click above.

Figure 24: IDM System Sign In Page

1.8 NPI Management

NPI Management allows Clearinghouse and Direct Provider Submitters to query, add, or terminate relationships with NPI numbers. Direct Provider Submitters may only perform this task at one NPI at a time using the NPI Management List feature. HETS Clearinghouse submitters have the option to utilize batch functionality to manage more than one NPI at a time via the NPI Batch Management feature. HETS Clearinghouse submitters can also download a list of active Medicare Provider/Supplier attestations associated with their organization.

To access the NPI Management feature, select ***NPI Management*** from either the menu or the display item on the HDT Application Site Map. Display options under NPI Management include ***NPI Management List*** and ***NPI Batch Management***. This is displayed in *Figure 25: HDT NPI Management Displaying Both Regular and Batch Options*.

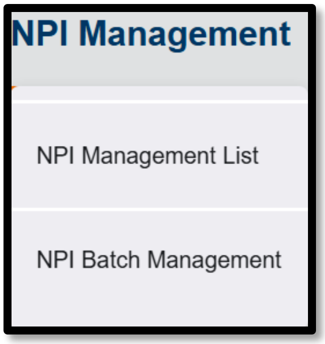


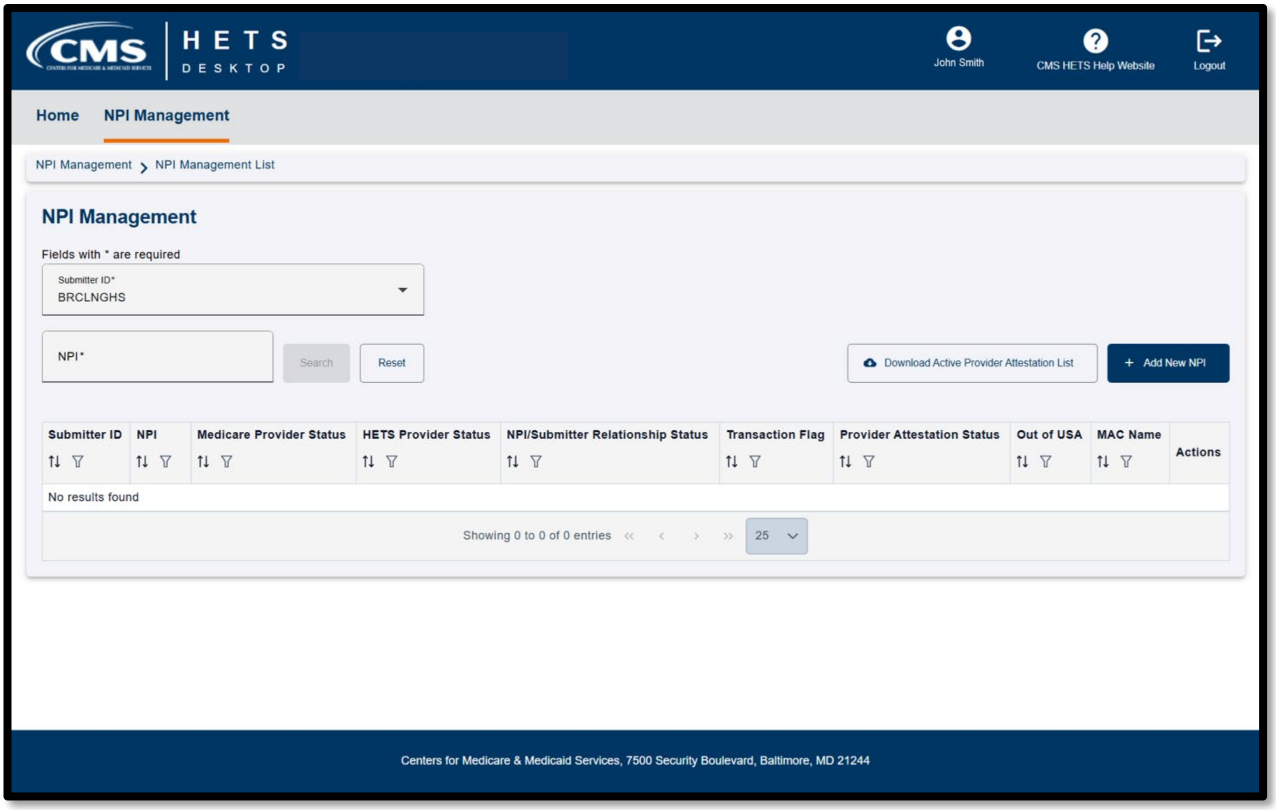
Figure 25: HDT NPI Management Displaying Both Regular and Batch Options

1.8.1 NPI Management List

NPI Management allows Clearinghouse and Direct Provider Submitters to query, add, or terminate relationships with NPI numbers one at a time.

Note: Data varies based on the user type. Some columns may not contain data.

To access the NPI Management List feature, select ***NPI Management*** from either the menu or the display item on the HDT Application Site Map, then choose ***NPI Management List***. The **NPI Management List** page is displayed in *Figure 26: NPI Management List Page*.



NPI Management

Fields with * are required

Submitter ID* BRCLNGHS

NPI*

Submitter ID	NPI	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag	Provider Attestation Status	Out of USA	MAC Name	Actions
No results found									

Showing 0 to 0 of 0 entries 25

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

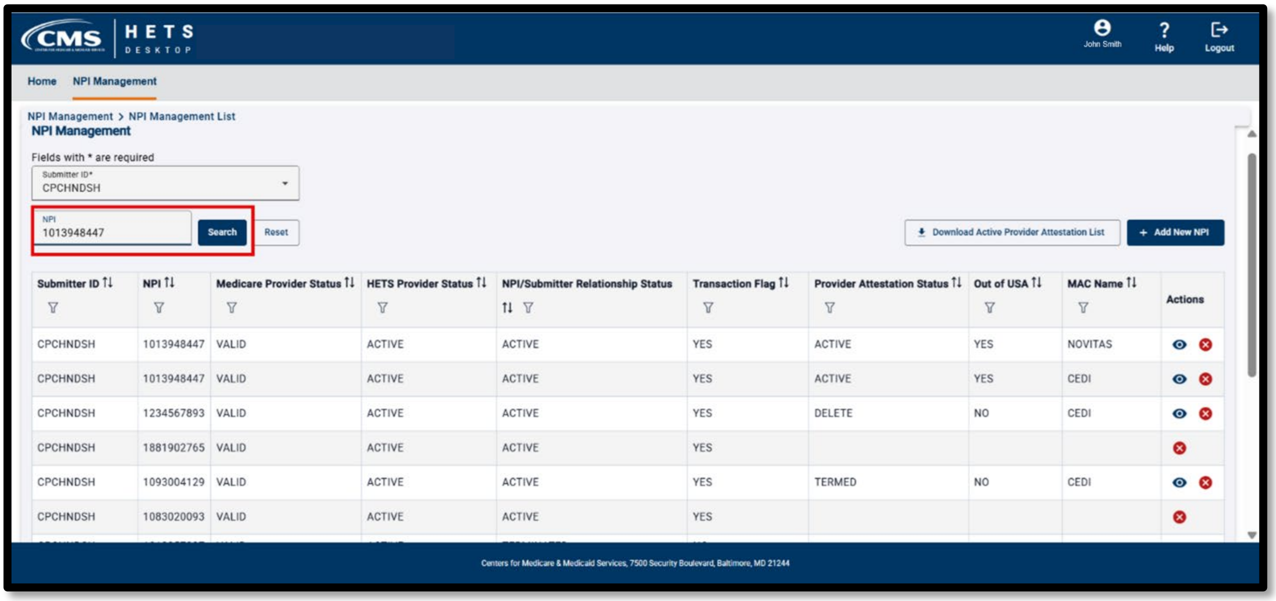
Figure 26: NPI Management List Page

By default, the NPI Management screen displays a table of data associated with the Submitter ID shown. Data is populated in this table from a mixture of HETS NPI/Submitter relationships and/or attestations. In the figure above, there are no HETS 270/271 relationships or attestations on file.

1.8.1.1 NPI Search

You can use NPI Search to determine the status of a particular NPI number in the HETS 270/271 system.

1. Select the appropriate HETS 270/271 Submitter ID from the drop-down menu (depending on the user and related organization, there may only be one value present).
2. Enter an NPI value in the NPI field (HDT only accepts numeric values in this field).
3. Select [Search] to query a specific NPI. The default search results are illustrated in *Figure 27: HDT NPI Management Screen – Search Results.*


CMS
HETS DESKTOP
John Smith
Help
Logout
Home
NPI Management
NPI Management > NPI Management List
Search
Reset
Download Active Provider Attestation List
+ Add New NPI
Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

NPI Management

Fields with * are required

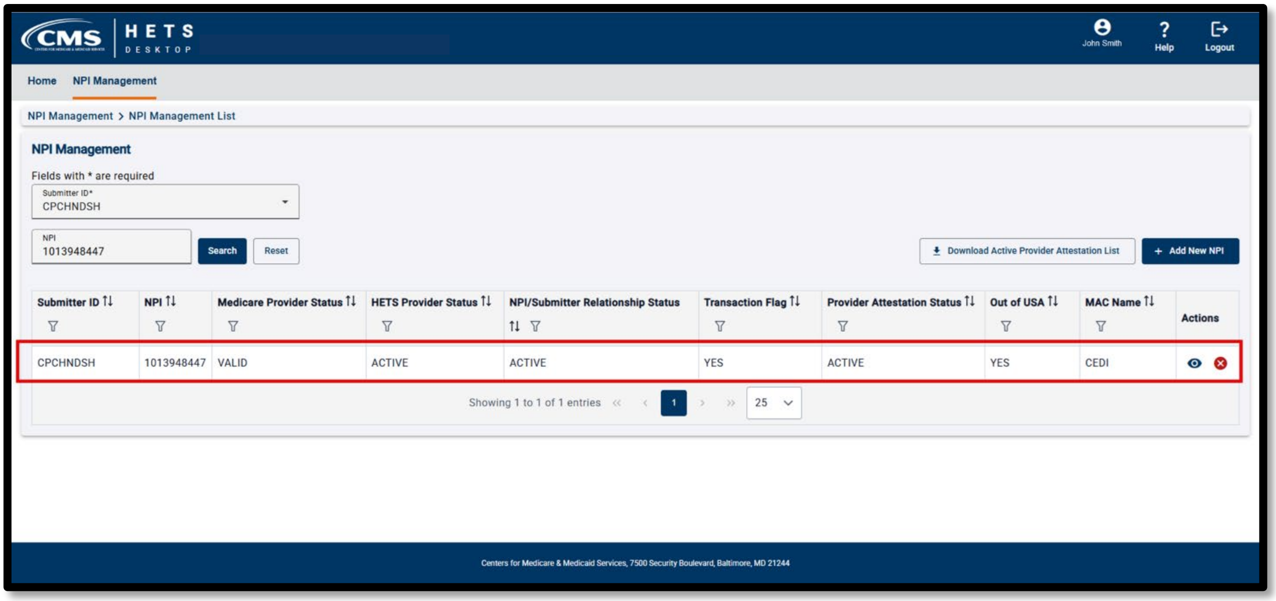
Submitter ID* CPCHNDSH

NPI 1013948447

Submitter ID	NPI	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag	Provider Attestation Status	Out of USA	MAC Name	Actions
CPCHNDSH	1013948447	VALID	ACTIVE	ACTIVE	YES	ACTIVE	YES	NOVITAS	👁 ⊗
CPCHNDSH	1013948447	VALID	ACTIVE	ACTIVE	YES	ACTIVE	YES	CEDI	👁 ⊗
CPCHNDSH	1234567893	VALID	ACTIVE	ACTIVE	YES	DELETE	NO	CEDI	👁 ⊗
CPCHNDSH	1881902765	VALID	ACTIVE	ACTIVE	YES				⊗
CPCHNDSH	1093004129	VALID	ACTIVE	ACTIVE	YES	TERMED	NO	CEDI	👁 ⊗
CPCHNDSH	1083020093	VALID	ACTIVE	ACTIVE	YES				⊗

Figure 27: HDT NPI Management Screen – Search Results

4. Results for requested actions are displayed in an NPI Results table, as illustrated in *Figure 28: HDT NPI Management Screen – NPI Entered Search Results*.



NPI Management > NPI Management List

NPI Management

Fields with * are required

Submitter ID*: CPCHNDSH

NPI: 1013948447

Submitter ID	NPI	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag	Provider Attestation Status	Out of USA	MAC Name	Actions
CPCHNDSH	1013948447	VALID	ACTIVE	ACTIVE	YES	ACTIVE	YES	CEDI	

Showing 1 to 1 of 1 entries

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 28: HDT NPI Management Screen – NPI Entered Search Results

Note: The table will display the results in the order in which the NPIs are entered into the NPI text box, with the most recent action listed first. The HDT application defaults to displaying up to 25 rows in the NPI Results table. The user can change this value in the entries drop-down to modify the results parameters.

The following information can appear in each column.

Note: Data varies based on the user type. Some columns may not contain data.

Table 2: NPI Management Screen Columns Description

Field Name	Field Description	Possible Values
Submitter ID	The 8-character Submitter ID selected by the user.	Organization HETS Submitter ID.
NPI	NPI entered by the user.	Medicare Provider or Supplier NPI.
Medicare Provider Status	This status indicates whether the NPI is an active, valid FFS Medicare Provider.	• Values include: • Valid: the Provider is an active, valid FFS Medicare Provider or Supplier. • Invalid: the Provider is not an active, valid FFS Medicare Provider or Supplier.

Field Name	Field Description	Possible Values
HETS Provider Status	This is the status of the NPI for the HETS 270/271 application	• Active: the NPI is active for the HETS 270/271 application. • Suspended: the NPI is suspended for the HETS 270/271 application. • Terminated: the NPI is terminated for the HETS 270/271 application. • Not Found: the NPI is not on file for the HETS 270/271 application.
NPI/Submitter Relationship Status	This is the status of the NPI/Submitter relationship for the HETS 270/271 application	• Active: the NPI/Submitter Relationship is active for the HETS 270/271 application. • Suspended: the NPI/Submitter Relationship is suspended for the HETS 270/271 application. • Terminated: the NPI/Submitter Relationship is terminated for the HETS 270/271 application. • Not Found: the NPI/Submitter Relationship is not on file for the HETS 270/271 application. • Expired: the NPI/Submitter Relationship is expired for the HETS 270/271 application.

Field Name	Field Description	Possible Values
Transaction Flag	This status flag indicates whether transactions with the HETS 270/271 application are permitted.	• Yes: Indicates that transactions with the HETS 270/271 application are permitted. This value is returned when all conditions are met:(Submitter Status = “Active”, AND Medicare Provider Status = “Valid”, AND HETS Provider Status = “Active”, AND NPI/Submitter Relationship Status = “Active”.) • No: Indicates that transactions with the HETS 270/271 application are not permitted. This value is returned when any of these conditions are met: • Submitter Status <> “Active”, OR • Medicare Provider Status <> “Valid”, OR • HETS Provider Status <> “Active”, OR • NPI/Submitter Relationship Status <> “Active”.

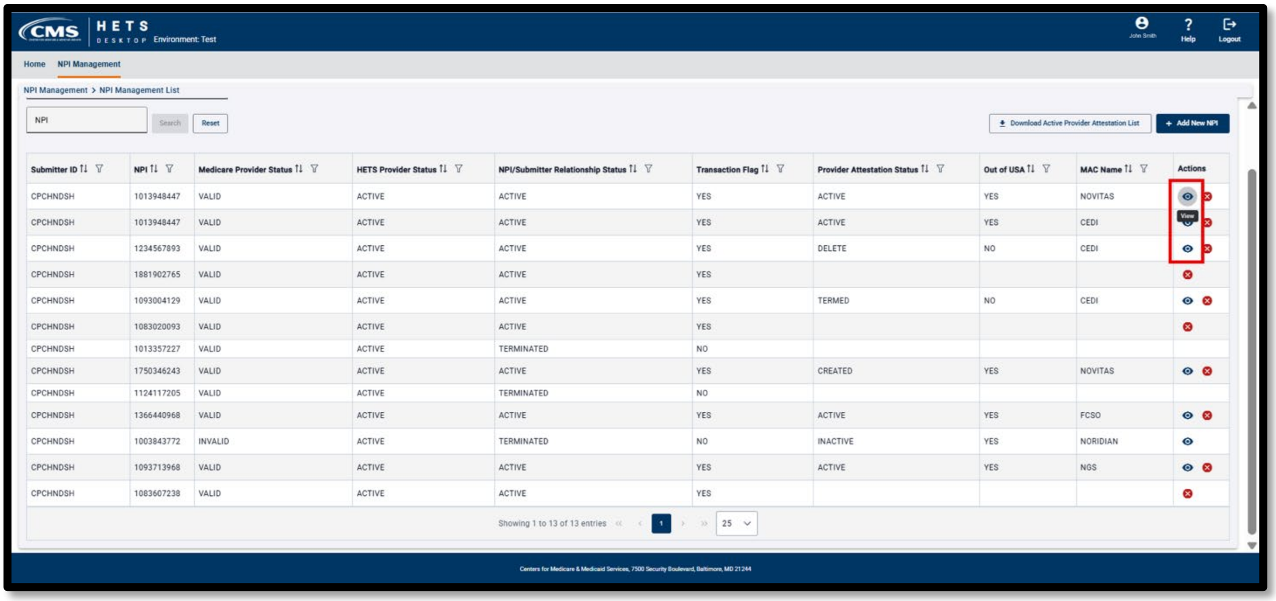
Field Name	Field Description	Possible Values
Provider Attestation Status	Viewable by clearinghouse submitters. If available, this column displays the status of any HETS EDI attestation created by the associated Medicare Provider or Supplier NPI as it relates to the clearinghouse's Submitter ID.	• Active: the NPI/Submitter attestation is active for the HETS 270/271 application. • Inactive: the NPI/Submitter attestation is no longer active for the HETS 270/271 application. • Terminated: the NPI/Submitter attestation has been terminated for the HETS 270/271 application. This status is typically used if a Medicare Provider or Supplier has not completed their required annual recertification of the HETS EDI attestation by the MAC's deadline. • Deleted: the NPI/Submitter attestation has been deleted by the Medicare Provider or Supplier. • Created: the NPI/Submitter attestation for the HETS 270/271 application has either a) just been created. Following an overnight update, this status will automatically update to 'Active' assuming that all other NPI/Submitter information is still eligible for use with HETS 270/271, or b) the NPI/Submitter attestation has a future effective date.
Out of USA	This value reflects the Medicare Provider or Supplier preference to the following question: "Do you allow organizations outside of the United States or its territories (offshore organizations) to use your NPIs to access eligibility data?" HDT displays this information if it is available on the attestation record.	Values (if present) are YES or NO.

Field Name	Field Description	Possible Values
MAC Name	This displays the name of the MAC used to create the associated attestation record.	• CEDI • CGS • FCSO • NGS • Noridian • Novitas • Palmetto • WPS
Actions	When appropriate, based on user role and usage, icons will appear in this column if the user has an actionable step.	• View: This allows clearinghouse submitter users to review the details of an attestation record by selecting the icon. • Terminate: This allows users to terminate an existing NPI/Submitter relationship by selecting the icon.

Table Notes: If the **Transaction Flag** displays a value of 'Yes', then the NPI can be successfully used to send a 270 request and potentially receive a complete 271 response with benefit information. Checking the Transaction Flag is the quickest and easiest way to determine if an NPI is set to use with HETS 270/271.

The **Provider Attestation Status, Out of USA, and MAC Name** columns in the table will only populate for Clearinghouse Submitter users. Direct Provider submitter users will not have access to this data.

5. If a Clearinghouse Submitter user wants to review the details of an existing attestation record that appears in their results table. In that case, they can select the 'View' icon when available. See *Figure 29: HDT NPI Management Screen – Attestation View*.



HETS DESKTOP Environment: Test
John Smith
Help
Logout
Home
NPI Management
NPI Management > NPI Management List
NPI
Search
Reset
Download Active Provider Attestation List
+ Add New NPI
View

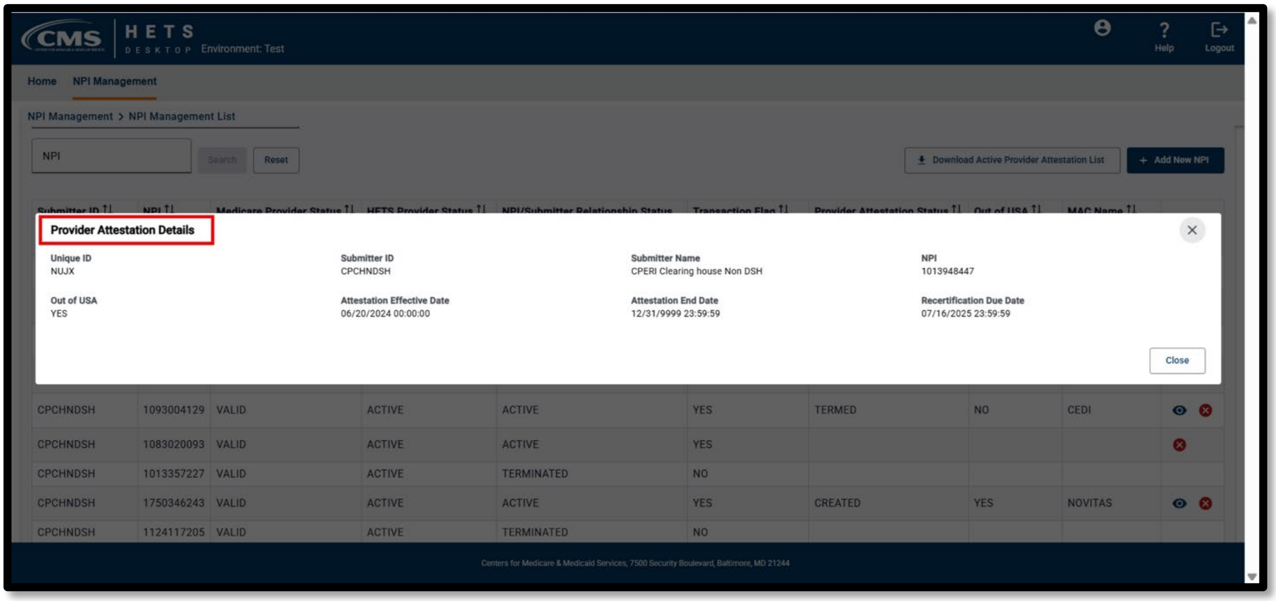
Submitter ID	NPI	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag	Provider Attestation Status	Out of USA	MAC Name	Actions
CPCHNDSH	1013948447	VALID	ACTIVE	ACTIVE	YES	ACTIVE	YES	NOVITAS	👁 ⊗
CPCHNDSH	1013948447	VALID	ACTIVE	ACTIVE	YES	ACTIVE	YES	CEDI	👁 ⊗
CPCHNDSH	1234567893	VALID	ACTIVE	ACTIVE	YES	DELETE	NO	CEDI	👁 ⊗
CPCHNDSH	1881902765	VALID	ACTIVE	ACTIVE	YES				⊗
CPCHNDSH	1093004129	VALID	ACTIVE	ACTIVE	YES	TERMED	NO	CEDI	👁 ⊗
CPCHNDSH	1083020093	VALID	ACTIVE	ACTIVE	YES				⊗
CPCHNDSH	1013357227	VALID	ACTIVE	TERMINATED	NO				
CPCHNDSH	1750346243	VALID	ACTIVE	ACTIVE	YES	CREATED	YES	NOVITAS	👁 ⊗
CPCHNDSH	1124117205	VALID	ACTIVE	TERMINATED	NO				
CPCHNDSH	1366440968	VALID	ACTIVE	ACTIVE	YES	ACTIVE	YES	FCSO	👁 ⊗
CPCHNDSH	1003843772	INVALID	ACTIVE	TERMINATED	NO	INACTIVE	YES	NORIDIAN	👁
CPCHNDSH	1093713968	VALID	ACTIVE	ACTIVE	YES	ACTIVE	YES	NGS	👁 ⊗
CPCHNDSH	1083607238	VALID	ACTIVE	ACTIVE	YES				⊗

Showing 1 to 13 of 13 entries 1 25

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 29: HDT NPI Management Screen – Attestation View

6. A pop-up screen will provide additional information about the attestation record. Select [X] at the upper right corner to close and continue. See *Figure 30: HDT NPI Management Screen – Attestation Detail View*.



HETS DESKTOP Environment: Test
Help
Logout
Home
NPI Management
NPI Management > NPI Management List
NPI
Search
Reset
Download Active Provider Attestation List
+ Add New NPI
×
Close

Provider Attestation Details

Unique ID NUJX	Submitter ID CPCHNDSH	Submitter Name CPERI Clearing house Non DSH	NPI 1013948447
Out of USA YES	Attestation Effective Date 06/20/2024 00:00:00	Attestation End Date 12/31/9999 23:59:59	Recertification Due Date 07/16/2025 23:59:59

Submitter ID	NPI	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag	Provider Attestation Status	Out of USA	MAC Name	
CPCHNDSH	1093004129	VALID	ACTIVE	ACTIVE	YES	TERMED	NO	CEDI	👁 ⊗
CPCHNDSH	1083020093	VALID	ACTIVE	ACTIVE	YES				⊗
CPCHNDSH	1013357227	VALID	ACTIVE	TERMINATED	NO				
CPCHNDSH	1750346243	VALID	ACTIVE	ACTIVE	YES	CREATED	YES	NOVITAS	👁 ⊗
CPCHNDSH	1124117205	VALID	ACTIVE	TERMINATED	NO				

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 30: HDT NPI Management Screen – Attestation Detail View

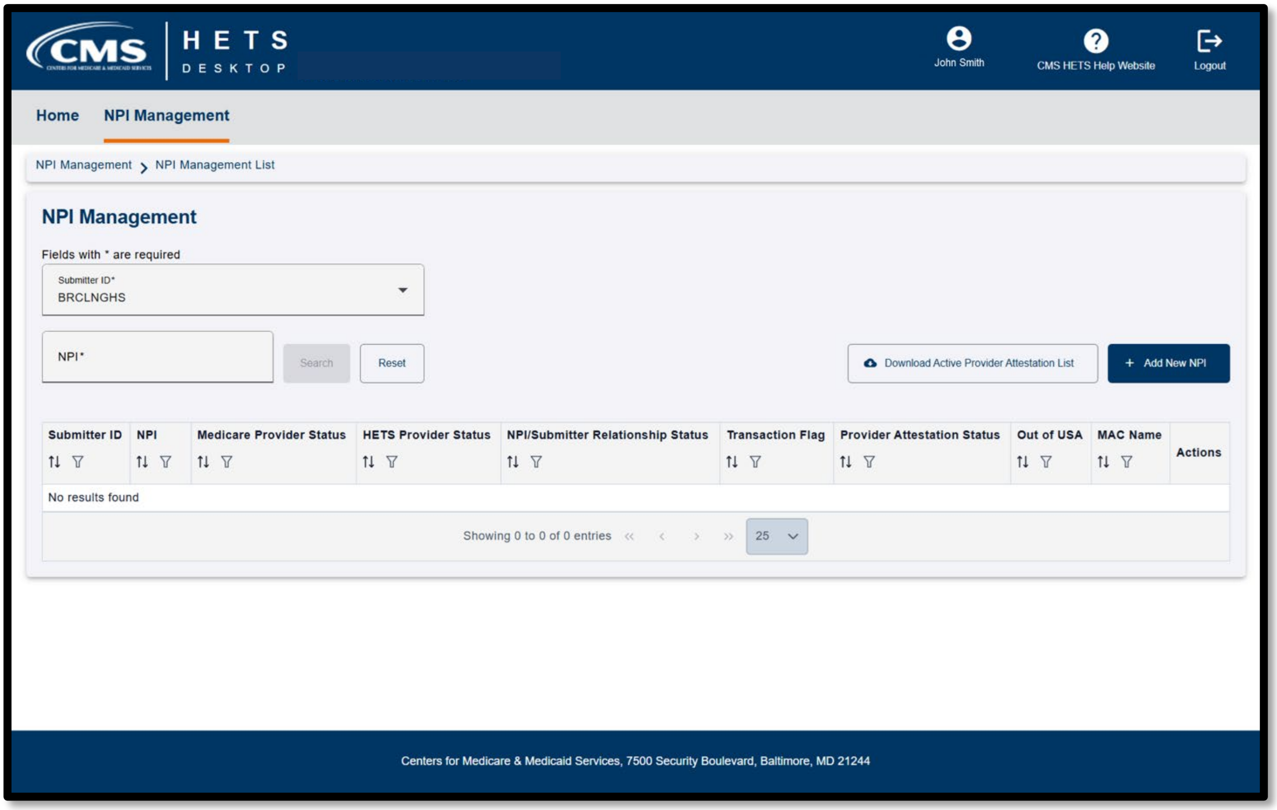
Note: The HETS Clearinghouse should direct any questions about the content of attestation data to the Medicare Provider or Supplier that created the attestation.

1.8.1.2 Add New NPI

The Add action establishes a relationship between a Submitter ID and an NPI, which is necessary for 270 request transactions to process successfully via the HETS 270/271 application. If users send an eligibility request with an NPI number that is not on file with CMS, is not a valid FFS Medicare Provider at the time the request is processed or is not associated with the Submitter. A 271 AAA error will be returned instead of entitlement information.

1.8.1.2.1 Action

To perform the Add action, follow these steps on the HDT User Interface NPI Management Screen, as illustrated in *Figure 31: HDT NPI Management Screen – Add*.



Submitter ID* BRCLNGHS

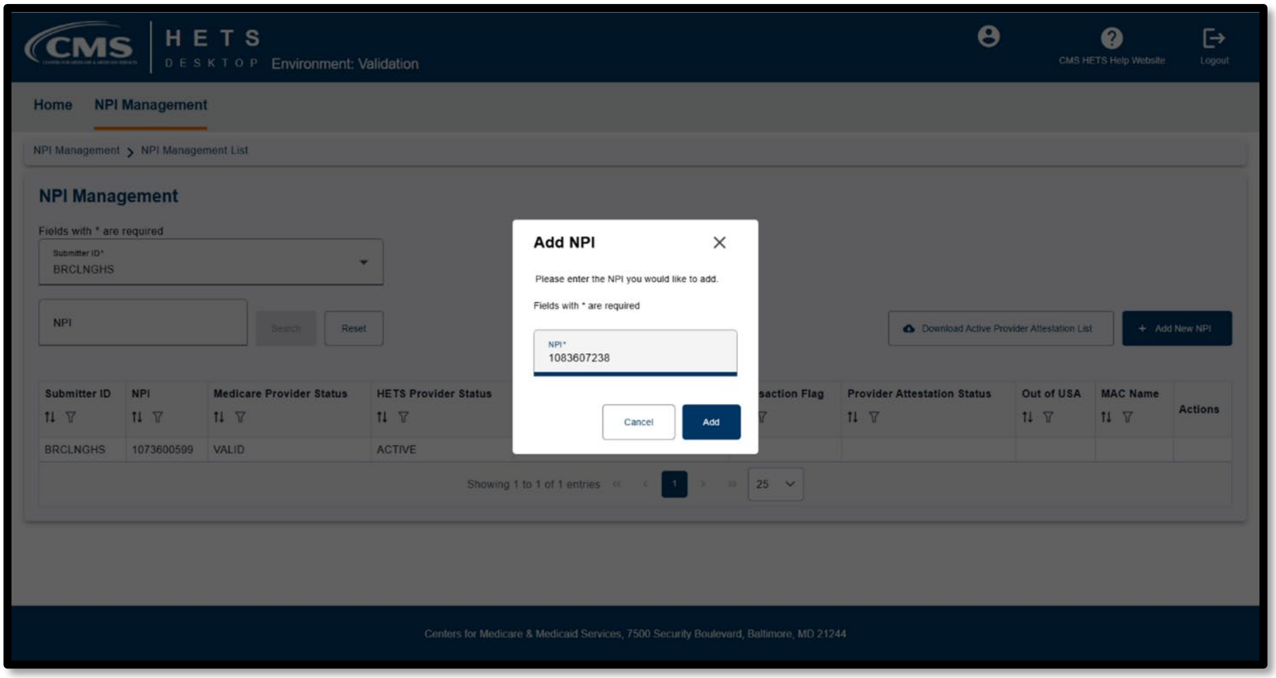
Submitter ID	NPI	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag	Provider Attestation Status	Out of USA	MAC Name	Actions
No results found									

Showing 0 to 0 of 0 entries 25

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 31: HDT NPI Management Screen – Add

1. Select a Submitter ID from the selection box labeled Submitter ID.
2. Select [+ Add New NPI].
3. An 'Add NPI' pop-up will appear. See *Figure 32: HDT NPI Management Screen – Add NPI*. Enter a 10-digit NPI number in the NPI field. HDT only accepts numeric values in the NPI field. Select [Add].


HETS DESKTOP
Environment: Validation
CMS HETS Help Website
Logout
Home
NPI Management
NPI Management > NPI Management List
Search
Reset
Download Active Provider Attestation List
+ Add New NPI
Cancel
Add
Showing 1 to 1 of 1 entries
1
25
Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

NPI Management

Fields with * are required

Submitter ID*: BRCLNGHS

NPI

Add NPI

Please enter the NPI you would like to add.

Fields with * are required

NPI*: 1083607238

Submitter ID	NPI	Medicare Provider Status	HETS Provider Status	saction Flag	Provider Attestation Status	Out of USA	MAC Name	Actions
BRCLNGHS	1073600599	VALID	ACTIVE					

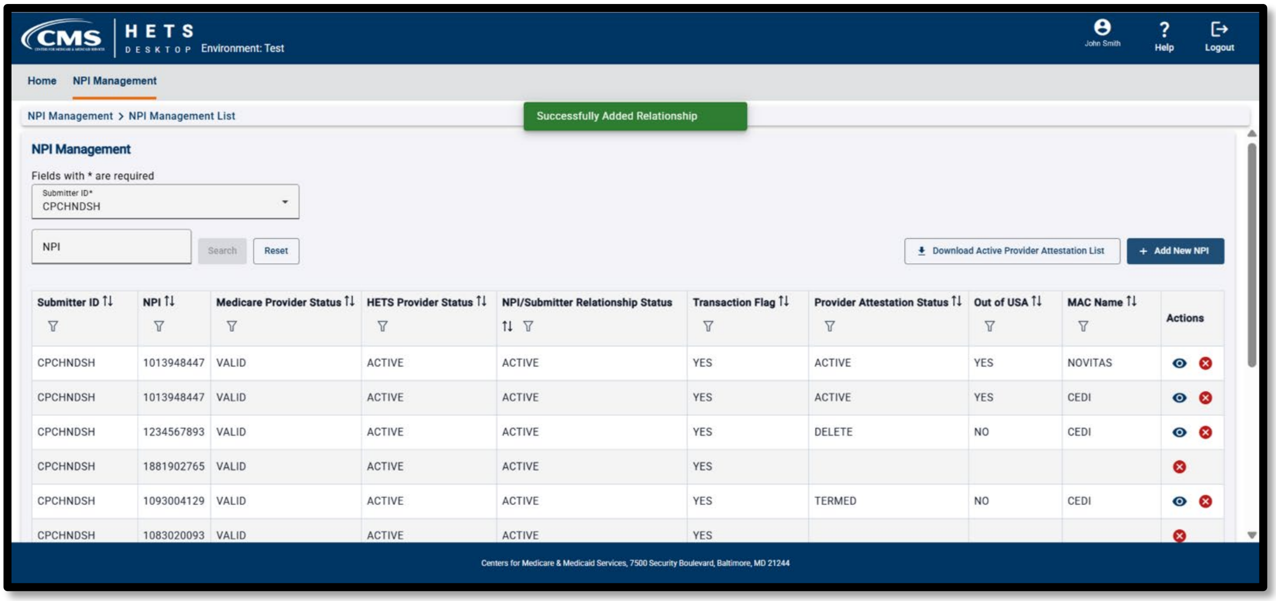
Figure 32: HDT NPI Management Screen – Add NPI

Note: The HDT application will clear the NPI field when users select an NPI Management action. The Submitter ID field will not be removed. If users wish to perform actions for a different Submitter ID associated with their Submitter Profile, they must select that Submitter ID from the Submitter ID drop-down list.

1.8.1.2.2 Result

1. HDT will display the status of the relationship add directly on the screen as a pop up. If a relationship was added, the table will also update with that result. Possible results are:
   - Successfully Added Relationship
   - Inactive Submitter Status (no relationship added)
2. Invalid Medicare Provider Status (no relationship added)
   - Relationship already exists (no relationship added)

Figure 33: HDT NPI Management Screen – Add NPI Results displays a status for the requested Add action.



NPI Management > NPI Management List

Successfully Added Relationship

NPI Management

Fields with * are required

Submitter ID*: CPCHNDSH

NPI

Submitter ID	NPI	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag	Provider Attestation Status	Out of USA	MAC Name	Actions
CPCHNDSH	1013948447	VALID	ACTIVE	ACTIVE	YES	ACTIVE	YES	NOVITAS	👁 ⊗
CPCHNDSH	1013948447	VALID	ACTIVE	ACTIVE	YES	ACTIVE	YES	CEDI	👁 ⊗
CPCHNDSH	1234567893	VALID	ACTIVE	ACTIVE	YES	DELETE	NO	CEDI	👁 ⊗
CPCHNDSH	1881902765	VALID	ACTIVE	ACTIVE	YES				⊗
CPCHNDSH	1093004129	VALID	ACTIVE	ACTIVE	YES	TERMED	NO	CEDI	👁 ⊗
CPCHNDSH	1083020093	VALID	ACTIVE	ACTIVE	YES				⊗

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 33: HDT NPI Management Screen – Add NPI Results Sample Responses

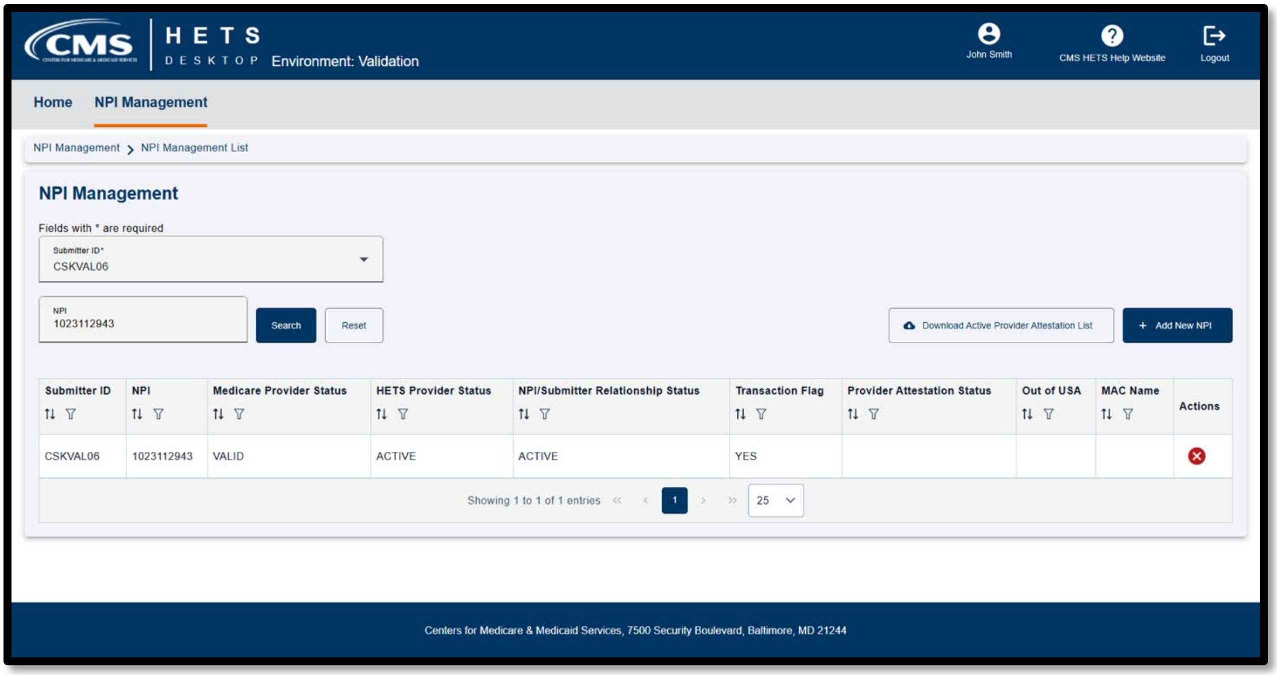
Note: After creating a new NPI/Submitter Relationship, the user should verify all components of that relationship's status, especially the Transaction Flag. HDT can add a new NPI/Submitter relationship and immediately suspend that relationship based on NPI and/or HETS Submitter status. Please verify that the Transaction Flag is set to YES before proceeding to send 270 requests with an NPI.

1.8.1.3 NPI Terminate

The Terminate action ends a relationship between a Submitter ID and an NPI when there is no longer a business relationship between them. Once a relationship is terminated, users will be unable to submit eligibility transactions via the HETS 270/271 application for the NPI.

1.8.1.3.1 Action

To perform the terminate action, follow these steps on the HDT NPI Management Screen, as illustrated in *Figure 34: HDT NPI Management Screen – Terminate Action*.



Environment: Validation

NPI Management

Fields with * are required

Submitter ID*: CSKVAL06

NPI: 1023112943

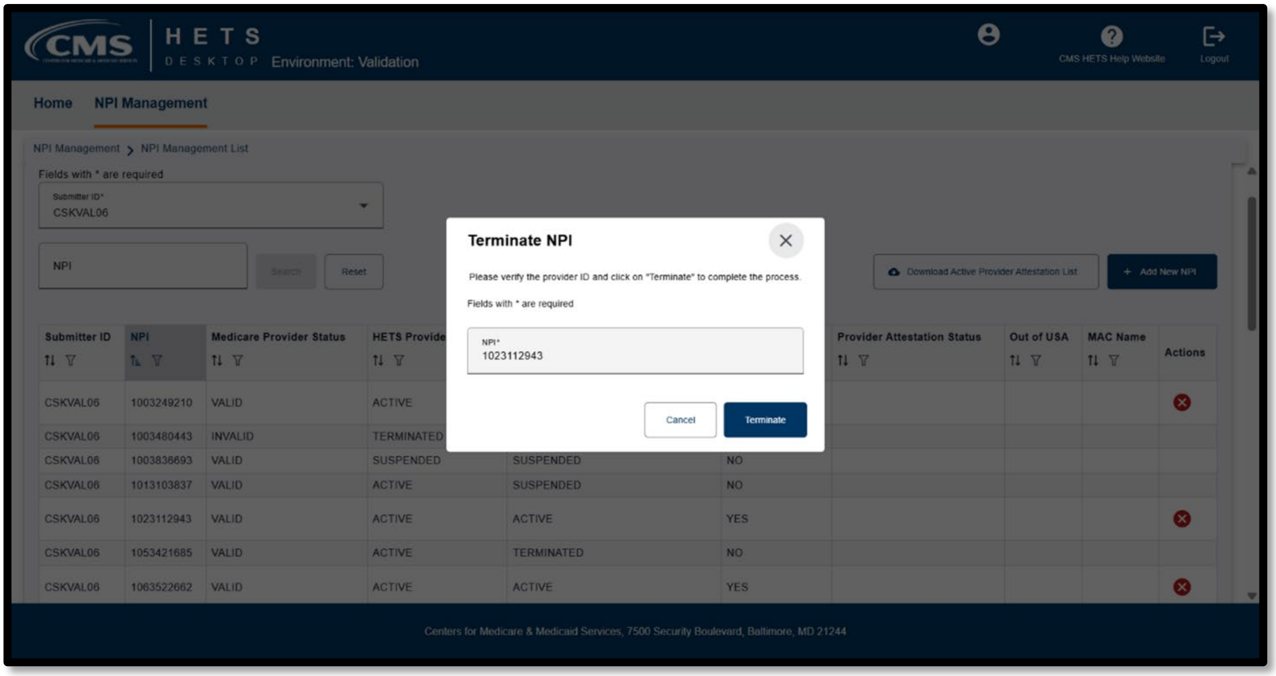
Submitter ID	NPI	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag	Provider Attestation Status	Out of USA	MAC Name	Actions
CSKVAL06	1023112943	VALID	ACTIVE	ACTIVE	YES				⊗

Showing 1 to 1 of 1 entries « ‹ 1 › » 25

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 34: HDT NPI Management Screen – Terminate Action

1. Select a Submitter ID from the selection box labeled Submitter ID.
2. Enter a 10-digit NPI number in the NPI field. HDT only accepts numeric values in the NPI field.
3. Select [Search].
4. The results page will display a row with the current NPI/Submitter Relationship Status. If the relationship is currently valid and active, with a Transaction Flag value of YES, the user will have the option to terminate the relationship if needed. To do so, the user would select the [X] icon to terminate the relationship.
5. A ‘Terminate NPI’ pop-up will appear. See *Figure 35: HDT NPI Management Screen – Terminate NPI Action*. Verify that the 10-digit NPI number in the NPI field is correct. HDT only accepts numeric values in the NPI field. Select [Terminate].


CMS
HETS DESKTOP Environment: Validation
CMS HETS Help Website
Logout
Home
NPI Management
NPI Management > NPI Management List
Search
Reset
Download Active Provider Attestation List
+ Add New NPI
Cancel
Terminate

Fields with * are required

Submitter ID* CSKVAL06

NPI

Terminate NPI

Please verify the provider ID and click on "Terminate" to complete the process.

Fields with * are required

NPI* 1023112943

Submitter ID	NPI	Medicare Provider Status	HETS Provide			Provider Attestation Status	Out of USA	MAC Name	Actions
CSKVAL06	1003249210	VALID	ACTIVE						⊗
CSKVAL06	1003480443	INVALID	TERMINATED						
CSKVAL06	1003836693	VALID	SUSPENDED	SUSPENDED	NO				
CSKVAL06	1013103837	VALID	ACTIVE	SUSPENDED	NO				
CSKVAL06	1023112943	VALID	ACTIVE	ACTIVE	YES				⊗
CSKVAL06	1053421685	VALID	ACTIVE	TERMINATED	NO				
CSKVAL06	1063522662	VALID	ACTIVE	ACTIVE	YES				⊗

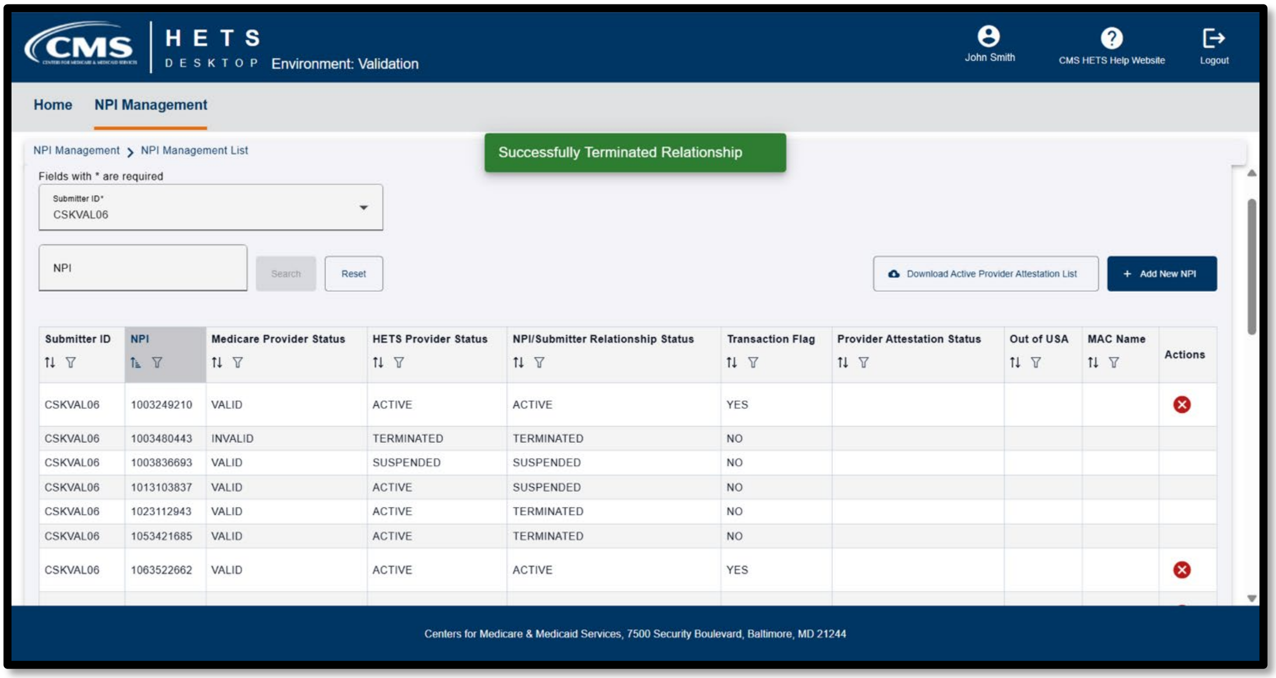
Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 35: HDT NPI Management Screen – Terminate NPI Action

1.8.1.3.2 Result

HDT will display the NPI relationship termination status directly on the screen as a pop-up, as well as update the value in the table. The only possible result for this action is a pop-up box reading “Successfully Terminated Relationship”; the table’s status for NPI/Submitter Relationship Status will change to ‘TERMINATED’. HDT only allows the Terminate action to be executed if the existing NPI/Submitter Relationship Status in the table is entirely valid and active, including a Transaction Flag value of ‘YES’.

Figure 36: HDT NPI Management Screen – Terminate Results displays the results for the terminate action.


CMS
HETS DESKTOP
Environment: Validation
John Smith
CMS HETS Help Website
Logout
Home
NPI Management
NPI Management > NPI Management List
Successfully Terminated Relationship
Search
Reset
Download Active Provider Attestation List
+ Add New NPI
Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Fields with * are required

Submitter ID*: CSKVAL06

NPI

Submitter ID	NPI	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag	Provider Attestation Status	Out of USA	MAC Name	Actions
CSKVAL06	1003249210	VALID	ACTIVE	ACTIVE	YES				⊗
CSKVAL06	1003480443	INVALID	TERMINATED	TERMINATED	NO				
CSKVAL06	1003836693	VALID	SUSPENDED	SUSPENDED	NO				
CSKVAL06	1013103837	VALID	ACTIVE	SUSPENDED	NO				
CSKVAL06	1023112943	VALID	ACTIVE	TERMINATED	NO				
CSKVAL06	1053421685	VALID	ACTIVE	TERMINATED	NO				
CSKVAL06	1063522662	VALID	ACTIVE	ACTIVE	YES				⊗

Figure 36: HDT NPI Management Screen – Terminate Results

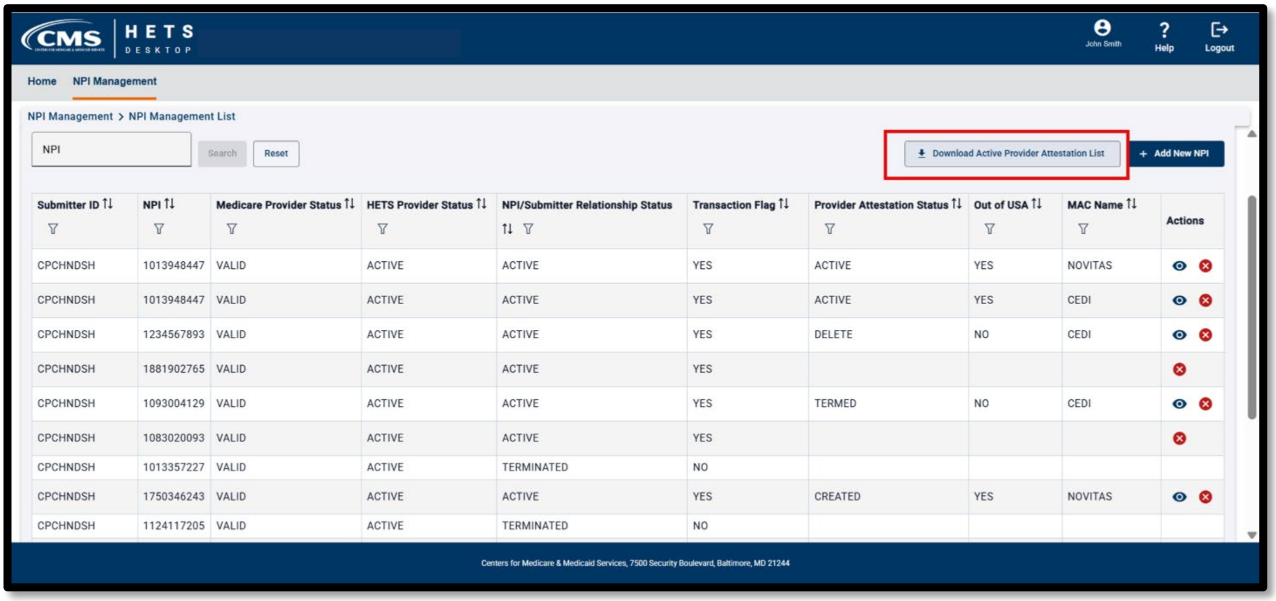
1.8.1.4 Download Active Provider Attestation List

Clearinghouse submitter users can download a list of HETS EDI attestations that are associated with their organization's HETS Unique ID. Medicare Providers and Suppliers across the country use the links provided on this webpage to create these HETS EDI attestations. Clearinghouse submitter users can download a current list of active HETS EDI attestations to their HETS Unique ID.

Please note that this report is a point-in-time data set. By comparing this list of active HETS EDI attestations obtained from HDT with your organization's list of Medicare eligibility customers, your organization can identify which of your customers still need to create attestations.

1.8.1.4.1 Action

Select [Download Active Provider Attestation List] from the NPI Management screen as illustrated in *Figure 37: Download Active Provider Attestation List*.



Submitter ID ⇅	NPI ⇅	Medicare Provider Status ⇅	HETS Provider Status ⇅	NPI/Submitter Relationship Status ⇅	Transaction Flag ⇅	Provider Attestation Status ⇅	Out of USA ⇅	MAC Name ⇅	Actions
CPCHNDSH	1013948447	VALID	ACTIVE	ACTIVE	YES	ACTIVE	YES	NOVITAS	👁 ⊗
CPCHNDSH	1013948447	VALID	ACTIVE	ACTIVE	YES	ACTIVE	YES	CEDI	👁 ⊗
CPCHNDSH	1234567893	VALID	ACTIVE	ACTIVE	YES	DELETE	NO	CEDI	👁 ⊗
CPCHNDSH	1881902765	VALID	ACTIVE	ACTIVE	YES				⊗
CPCHNDSH	1093004129	VALID	ACTIVE	ACTIVE	YES	TERMED	NO	CEDI	👁 ⊗
CPCHNDSH	1083020093	VALID	ACTIVE	ACTIVE	YES				⊗
CPCHNDSH	1013357227	VALID	ACTIVE	TERMINATED	NO				
CPCHNDSH	1750346243	VALID	ACTIVE	ACTIVE	YES	CREATED	YES	NOVITAS	👁 ⊗
CPCHNDSH	1124117205	VALID	ACTIVE	TERMINATED	NO				

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 37: Download Active Provider Attestation List

1.8.1.4.2 Result

A comma-separated file named "Active_Provider_Attestation_Report-XXXXXXXX" (where your organization's HETS Submitter ID is the suffix) will download to your machine's default downloads location. The file will contain the following information when available (see *Table 2: NPI Management Screen Columns Description* for additional information about possible values in some of these fields):

- Unique ID
- Submitter ID
- Submitter Name
- NPI
- Provider Name
- Provider Attestation Status
- Out of USA
- Attestation Effective Date
- Attestation End Date
- Recertification Due Date
- MAC Name

Note: The HETS Clearinghouse should direct any questions about the content of attestation data to the Medicare Provider or Supplier that created the attestation.

1.9 NPI Batch Management

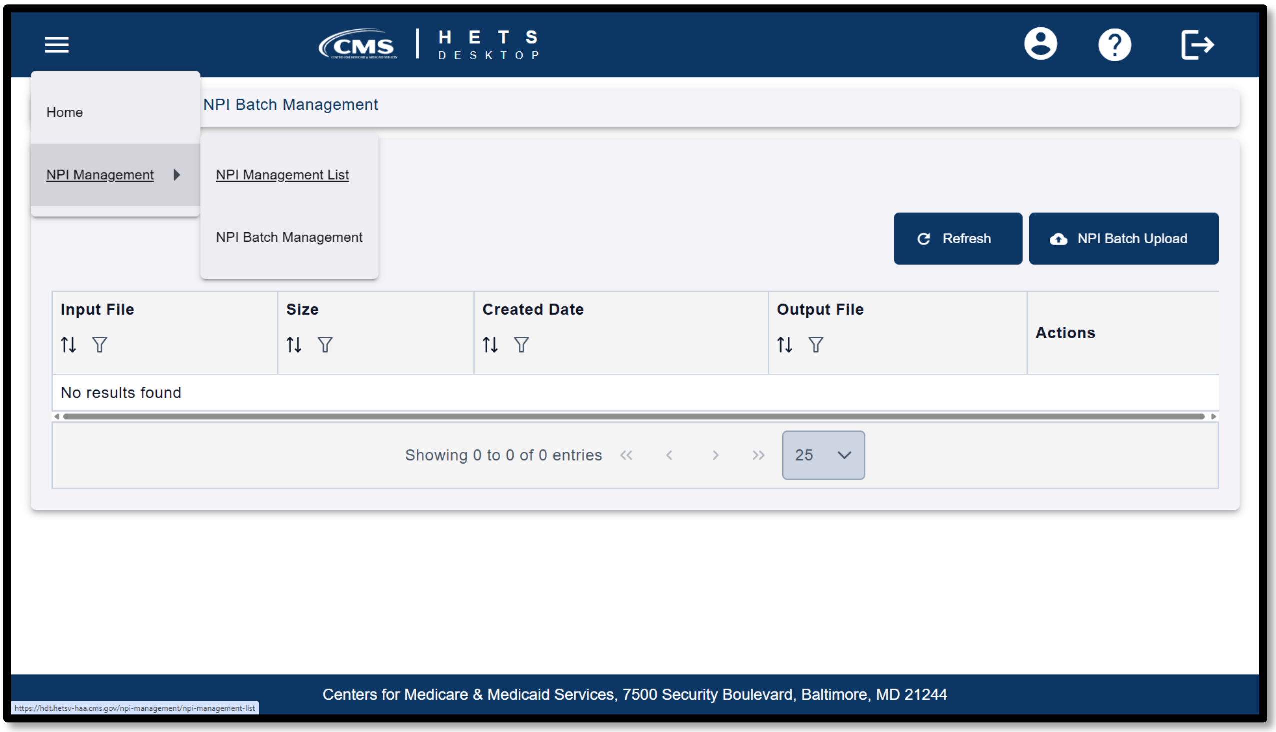
NPI Batch Management is available only to Clearinghouse Submitters. This feature enables users to query, add, and/or terminate relationships associated with multiple NPI numbers simultaneously.

The NPI Batch Management screen allows users to complete the following:

- NPI Batch Upload
- File Download
- View uploaded files
- View processed files
- Cancel actions

Note: Clearinghouse Submitters are limited to uploading only one batch file per day. If a Clearinghouse Submitter attempts to upload more than one file during a single calendar day, an error message is returned in the batch output file.

To access the NPI Management feature, select [NPI Batch Management] in the navigation menu as illustrated in *Figure 38: NPI Batch Management Navigation* below.



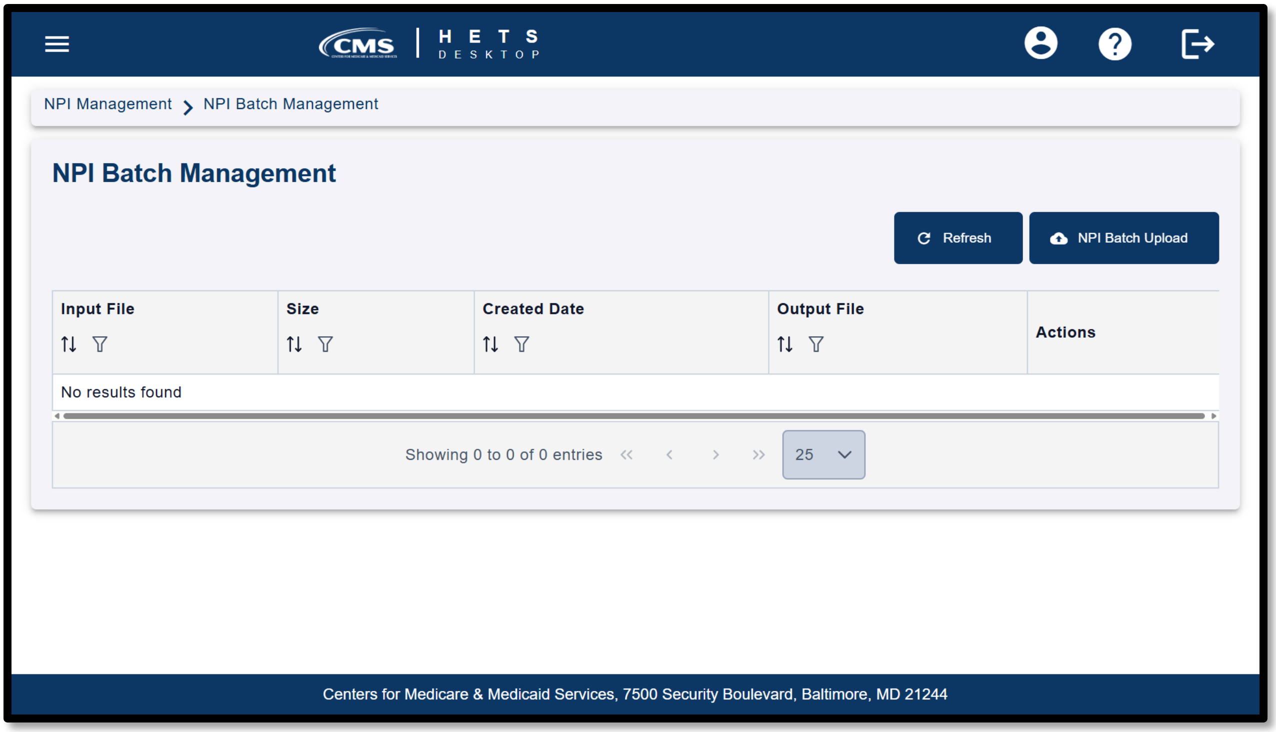
Input File	Size	Created Date	Output File	Actions
No results found				

Showing 0 to 0 of 0 entries

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 38: NPI Batch Management Navigation

The HDT NPI Batch Management Screen displays as described in *Figure 39: NPI Batch Management Page*.



Input File	Size	Created Date	Output File	Actions
No results found				

Showing 0 to 0 of 0 entries

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 39: NPI Batch Management Page

1.9.1 Batch File Layout

1.9.1.1 Input File

The required naming convention for the batch input file is:

SubmitterID.IN.HDT.EFT

Customizable elements:

SubmitterID = The HETS Submitter ID assigned to your organization by CMS. (Example: C123A456).

All other file name elements are required and constant.

Sample input file name: File Name: C123A456.IN.HDT.EFT

The acceptable file format for the NPI Batch Management input file is a comma-delimited, flat text file. The input file consists of three data elements per line – Submitter ID, NPI, and Action. Refer to the Input File Layout and a description of elements.

Table 3: Input File Layout and Element Description

Data Element	Data Type	Length	Possible Values	Description
Submitter ID	Alphanumeric	8	N/A	The 8-character Submitter ID associated with the Clearinghouse.
NPI	Numeric	10	N/A	The 10-digit NPI to which the Clearinghouse sends eligibility transactions for the HETS 270/271 application.
Action	Alpha	1	Q, A, or T	The action requested by the Clearinghouse to query the status of, to add, or to terminate a relationship with an NPI. Values include: Q: Request a query of the relationship between the Submitter ID and the NPI. A: Request to add a relationship between the Submitter ID and the NPI. T: Request to terminate the relationship between the Submitter ID and the NPI.

Sample Input File

File Name: C123A456.IN.HDT.EFT

```
C123A456,1111111111,Q
C123A456,2222222222,Q
C123A456,3333333333,A
C123A456,3333333333,A
C123A456,4444444444,A
C123A456,5555555555,A
C123A456,6666666666,T
C123A456,6666666666,T
C123A456,7777777777,T
```

1.9.1.2 Output File

The system-generated naming convention for the batch output file is:

SubmitterID.OUT.HDT.EFT.D{date}.T{time}

System-defined elements:

SubmitterID = The HETS Submitter ID assigned to your organization by CMS.

Dyymmdd = {Date} in yymmdd format

Thhmmsst – {Time} in hhmmsst format

All other file name elements are required and constant.

Sample output file name: File Name: C123A456.OUT.HDT.EFT.D200401.T0122331

The output file generated by the HDT application will be in the same format as the input file, with the addition of a date and time stamp indicating when the file was processed, and status responses appended to each line.

If the NPI Batch Management input file contains an NPI that is not 10 characters long or is not numeric, the output file will include a row for the NPI with a Medicare Provider Status of 'Invalid'. All rows within an input file will be processed if there are no batch file errors.

Refer to *Table 4: Output File Layout* and a description of elements.

Table 4: Output File Layout

Data Element	Data Type	Possible Values	Description
Submitter ID	Alphanumeric	N/N/AA	The 8-character Submitter ID associated with the Clearinghouse.
NPI	Numeric	N/A	The NPI that the Clearinghouse provided on the input file.
Action Requested	Alpha	Q, A, or T	The action requested by the Submitter on the input file for the NPI. Values include: Q: Request a query of the relationship between the Submitter ID and the NPI. A: Request to add a relationship between the Submitter ID and the NPI. T: Request to terminate the relationship between the Submitter ID and the NPI.

Data Element	Data Type	Possible Values	Description
Action Result	Alpha	Q, A, AE, SP, IM, T, AT, NE, or VA	The result of the action requested by the Submitter on the input file for the NPI. Values include: Q: The query request has been processed, and the query results are displayed. A: The NPI/Submitter relationship has been added to the HDT application. AE: The NPI/Submitter relationship already exists and cannot be added. SP: The NPI/Submitter relationship is currently suspended and cannot be added. IM: The Medicare Provider Status is invalid and cannot be added. T: The NPI/Submitter relationship has been terminated in the HDT application. AT: The NPI/Submitter relationship is already terminated and cannot be terminated. NE: The NPI/Submitter relationship does not exist and cannot be terminated. VA: No Relationship with VA – the NPI/Submitter relationship cannot be added as the NPI belongs to a VA facility.
Submitter Status	Alpha	A, S or T	The status of the Submitter in the HDT application. Values include: **A**: **Active** and authorized for HETS. **S**: **Suspended** and not authorized for HETS. Please contact MCARE for additional information. **T**: **Terminated** Submitter. Please contact MCARE for additional information.
Medicare Provider Status	Alpha	V or I	The status that indicates whether the NPI is an active, valid FFS Medicare Provider. Values include: V: The NPI is an active, valid FFS Medicare Provider. I: The NPI is not an active, valid FFS Medicare Provider.

Data Element	Data Type	Possible Values	Description
HETS Provider Status	Alpha	A, S, T or NF	The status of the NPI for the HETS 270/271 application. Values include: A: The NPI is active for the HETS 270/271 application. S: The NPI is suspended for the HETS 270/271 application. T: The NPI is terminated for the HETS 270/271 application. NF: The NPI is not on file for the HETS 270/271 application.
NPI/Submitter Relationship Status	Alpha	A, S, T, NF, or E	The status of the NPI/Submitter relationship for the HETS 270/271 application. Values include: A: The NPI/Submitter Relationship is active for the HETS 270/271 application. S: The NPI/Submitter Relationship is suspended for the HETS 270/271 application. T: The NPI/Submitter Relationship is terminated for the HETS 270/271 application. NF: The NPI/Submitter Relationship is not on file for the HETS 270/271 application. E: The NPI/Submitter Relationship expired for the HETS 270/271 application.
Transaction Flag	Alpha	Y or N	The status flag indicates whether transactions with the HETS 270/271 application are permitted. Values include: Y: Yes, transactions with the HETS 270/271 application are permitted. This value is returned when the following conditions are met: Submitter Status = A; and Medicare Provider Status = V; and HETS Provider Status = A; and NPI/Submitter Relationship Status = A N: No, transactions with the HETS 270/271 application are not permitted.

Sample Output File

File Name: C123A456.OUT.HDT.EFT,D200401.T0122331

File processed on 04/01/2020 01:22 AM

```
C123A456,1111111111,Q,Q,A,V,A,A,Y
C123A456,2222222222,Q,Q,A,I,T,T,N
```

C123A456,3333333333,A,A,A,V,A,A,Y

C123A456,3333333333,A,AE,A,V,A,A,Y

C123A456,4444444444,A,SP,A,V,S,S,N

C123A456,5555555555,A,IM,A,I,NF,NF,N

C123A456,6666666666,T,T,A,V,A,T,N

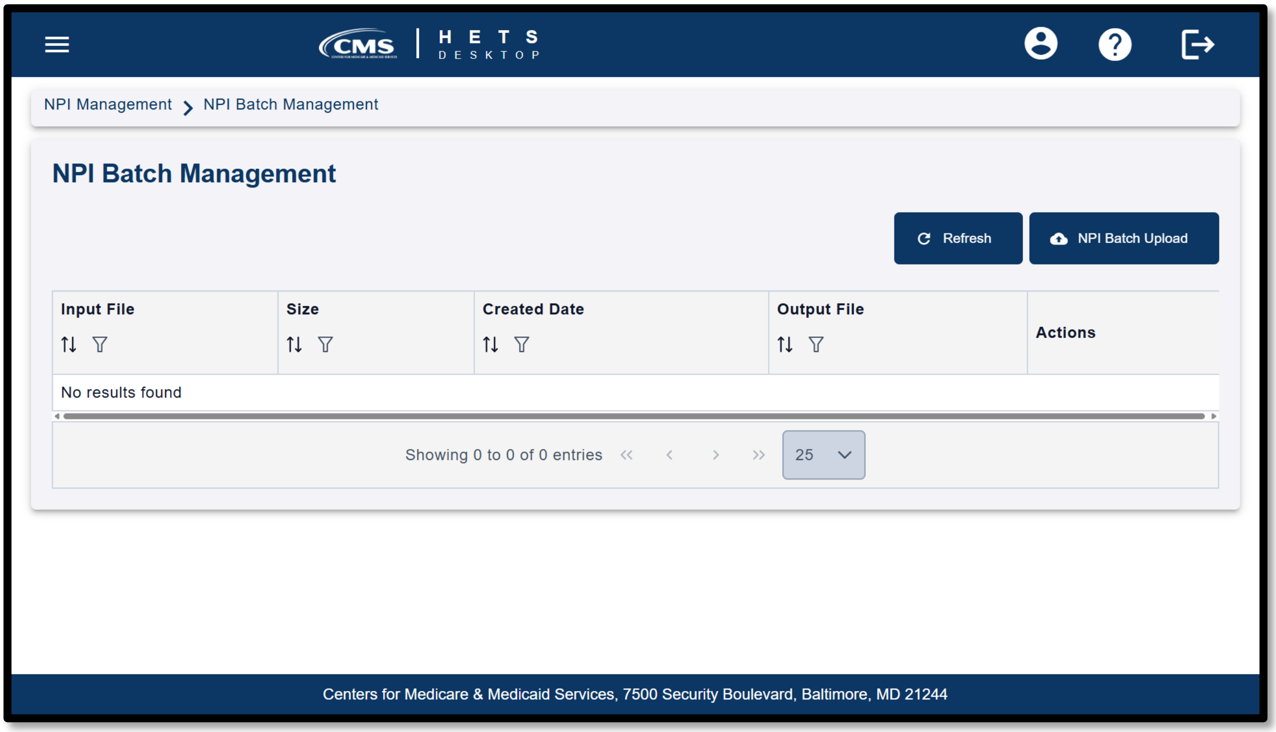
C123A456,6666666666,T,AT,A,V,A,T,N

C123A456,7777777777,T,NE,A,I,NF,NF,N

Note: The Sample Input and Output Files are for illustrative purposes only. Actual results will vary based on the status of NPIs and Submitter IDs in the HDT application.

1.9.2 Using NPI Batch Management

This is the initial landing page in the batch file section. It will display recent batch files and their results. The HDT NPI Batch Management Screen will display as illustrated in *Figure 40: HDT NPI Batch Management Screen*.



NPI Batch Management

Input File	Size	Created Date	Output File	Actions
No results found				

Showing 0 to 0 of 0 entries

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 40: HDT NPI Batch Management Screen

1.9.2.1 Uploading a File

To upload an input file, follow these steps:

1. On the HDT NPI Batch Management screen, illustrated above, select [NPI Batch Upload]. A pop-up will open as illustrated by *Figure 41: Select Upload File for Processing* and allow you to select the file from your local device.

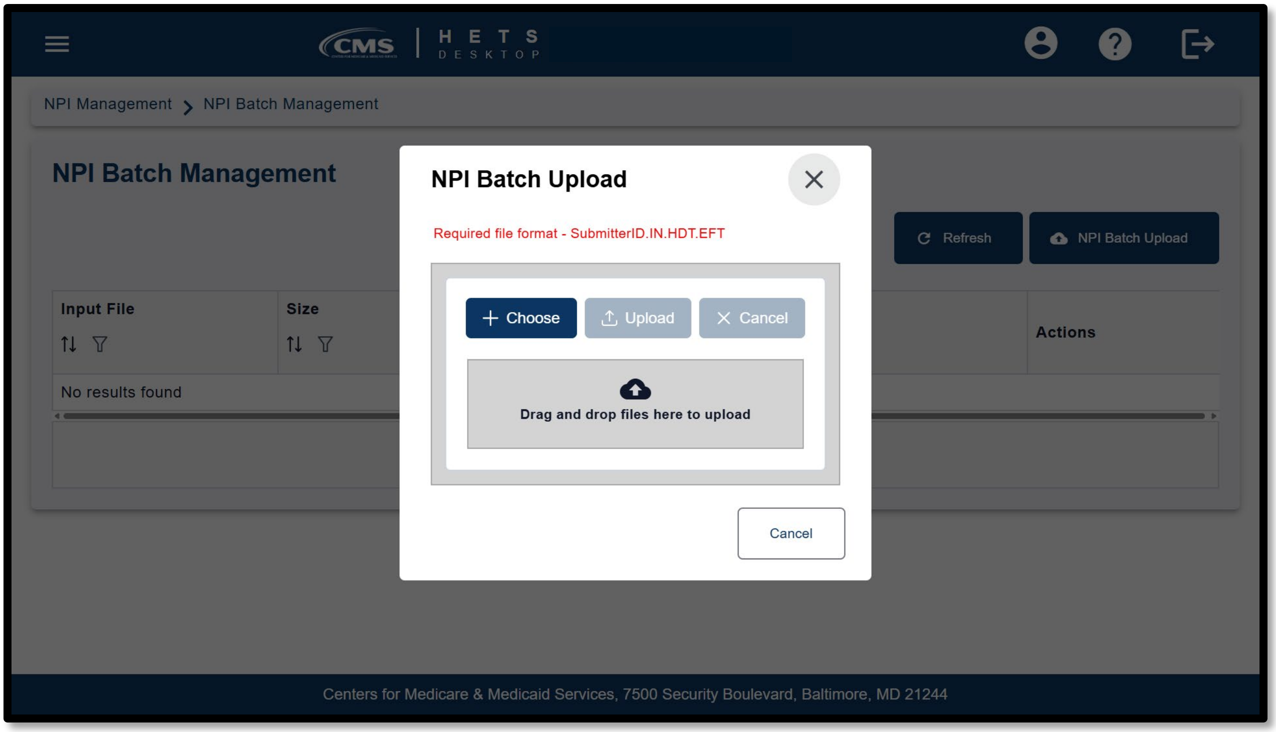

H E T S
D E S K T O P
NPI Management > NPI Batch Management
NPI Batch Management
Refresh
NPI Batch Upload
Input File
Size
Actions
No results found
NPI Batch Upload
Required file format - SubmitterID.IN.HDT.EFT
Choose
Upload
Cancel
Drag and drop files here to upload
Cancel
Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 41: Select Upload File for Processing

2. Select the comma-delimited, flat text file containing the multiple NPI relationships you wish to query, add, and/or terminate. Then select [Open]. See *Figure 42: Upload File Selected*.

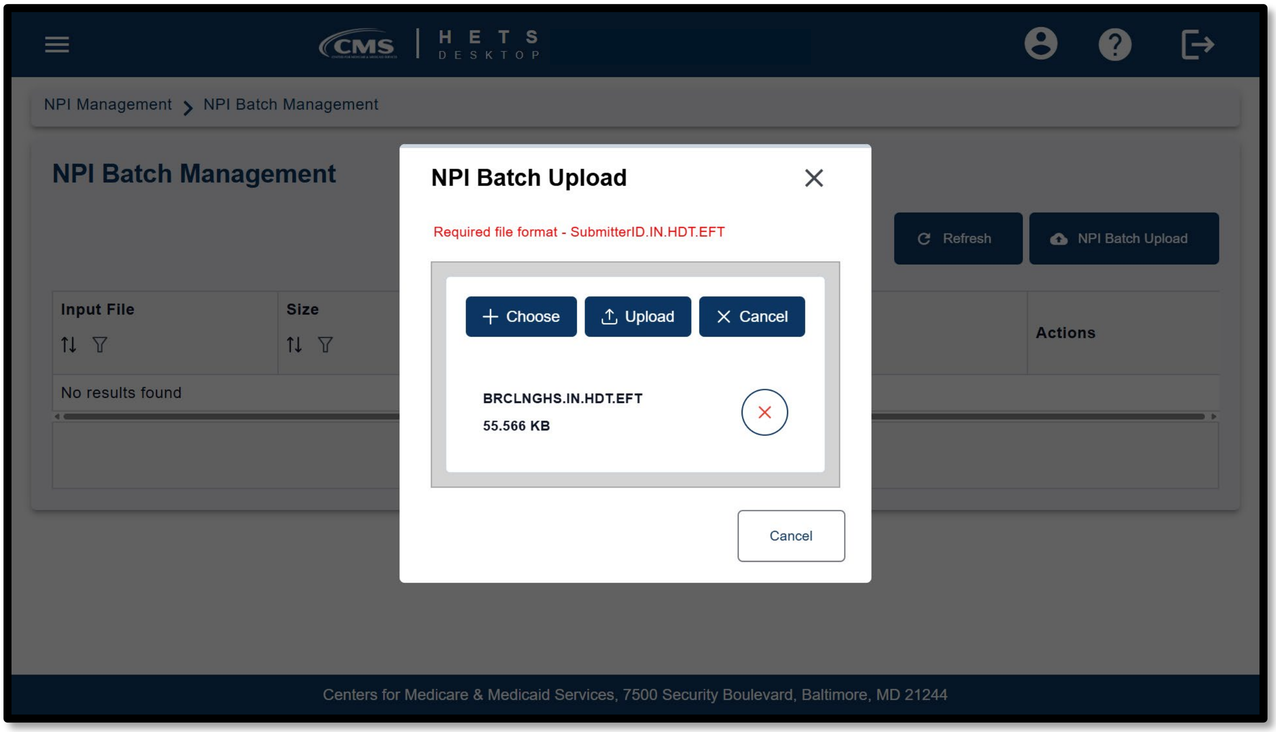
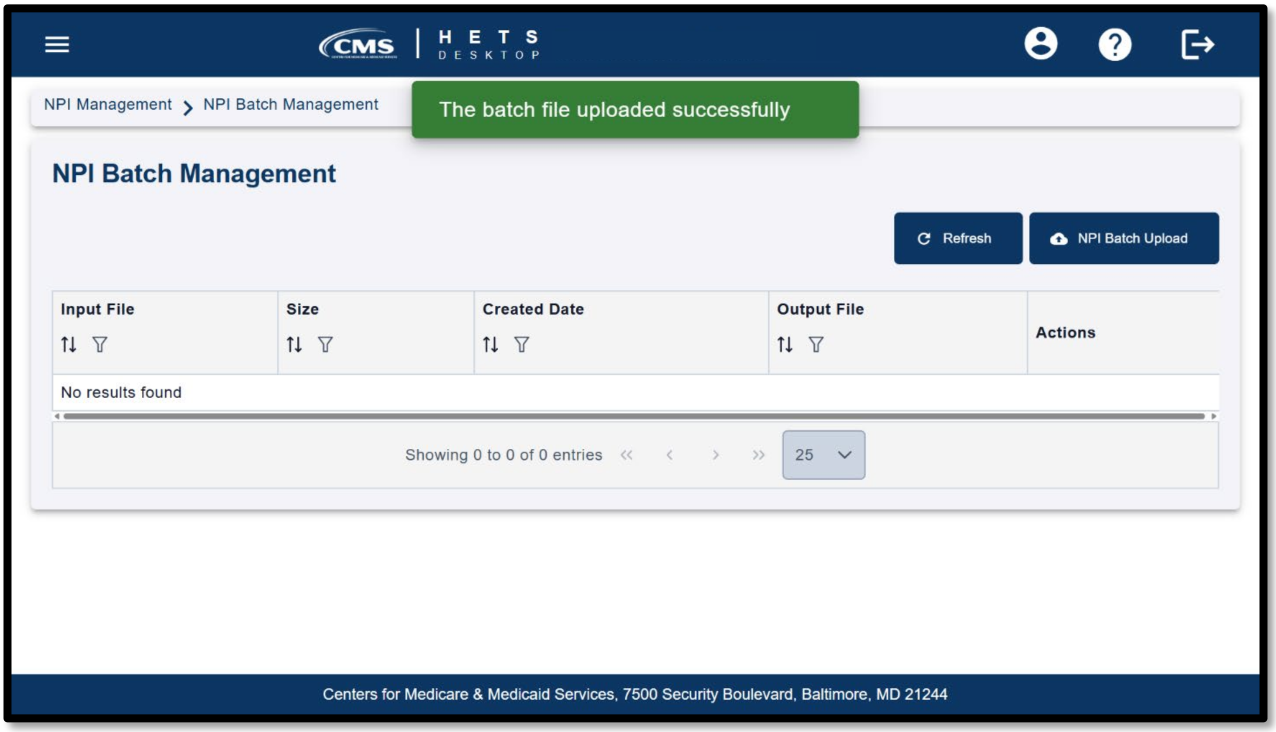

H E T S
D E S K T O P
NPI Management > NPI Batch Management
NPI Batch Management
Refresh
NPI Batch Upload
Input File
Size
Actions
No results found
NPI Batch Upload
Required file format - SubmitterID.IN.HDT.EFT
Choose
Upload
Cancel
BRCLNGHS.IN.HDT.EFT
55.566 KB
Cancel
Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 42: Upload File Selected

3. Select [Upload]. Once the file has finished uploading, HDT will display the message “The batch file uploaded successfully.” See *Figure 43: Batch File Submitted*.



The batch file uploaded successfully

NPI Batch Management

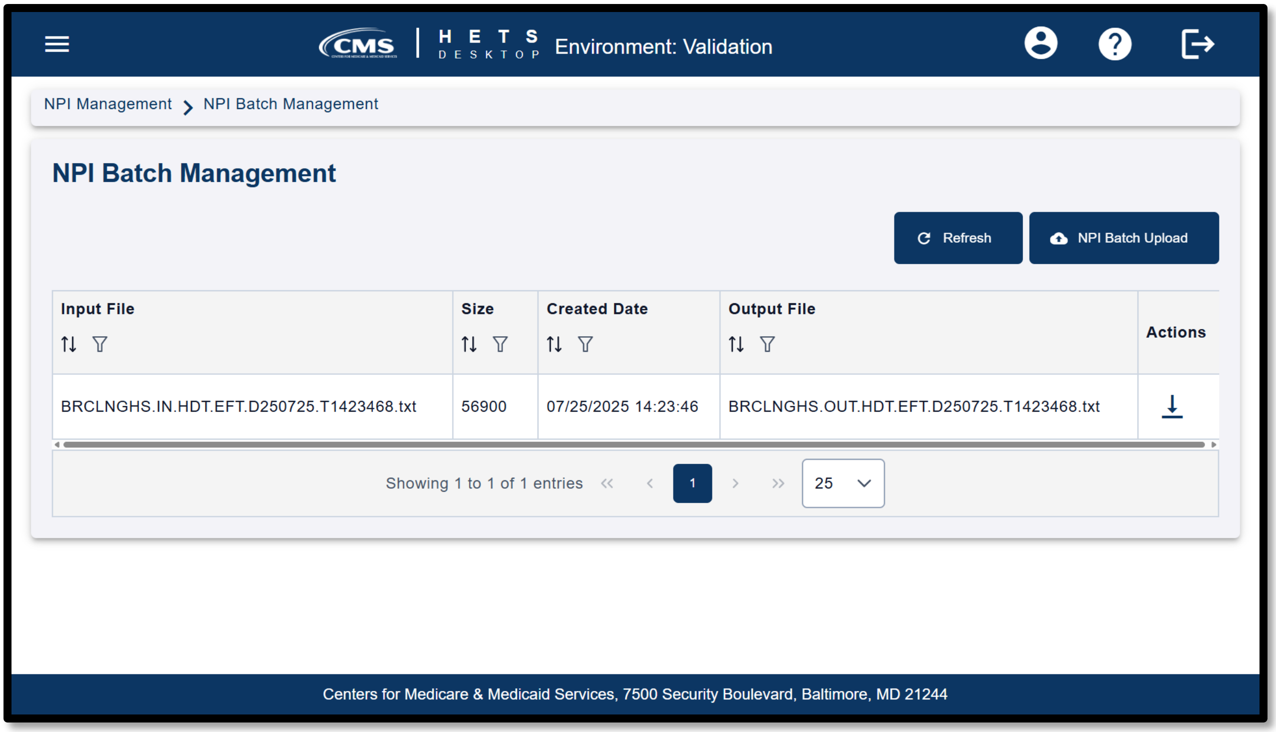
Input File	Size	Created Date	Output File	Actions
No results found				

Showing 0 to 0 of 0 entries

Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

Figure 43: Batch File Submitted

4. The screen will also update to show the file in process, as illustrated in *Figure 43: Batch File Submitted*. Recent batch files will display essential details, including input file name, file size, created date, and if available, output file name. Completed batch files will have a Download file action available.


CMS
HETS DESKTOP
Environment: Validation
NPI Management > NPI Batch Management
Refresh
NPI Batch Upload
Showing 1 to 1 of 1 entries
1
25
Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

NPI Batch Management

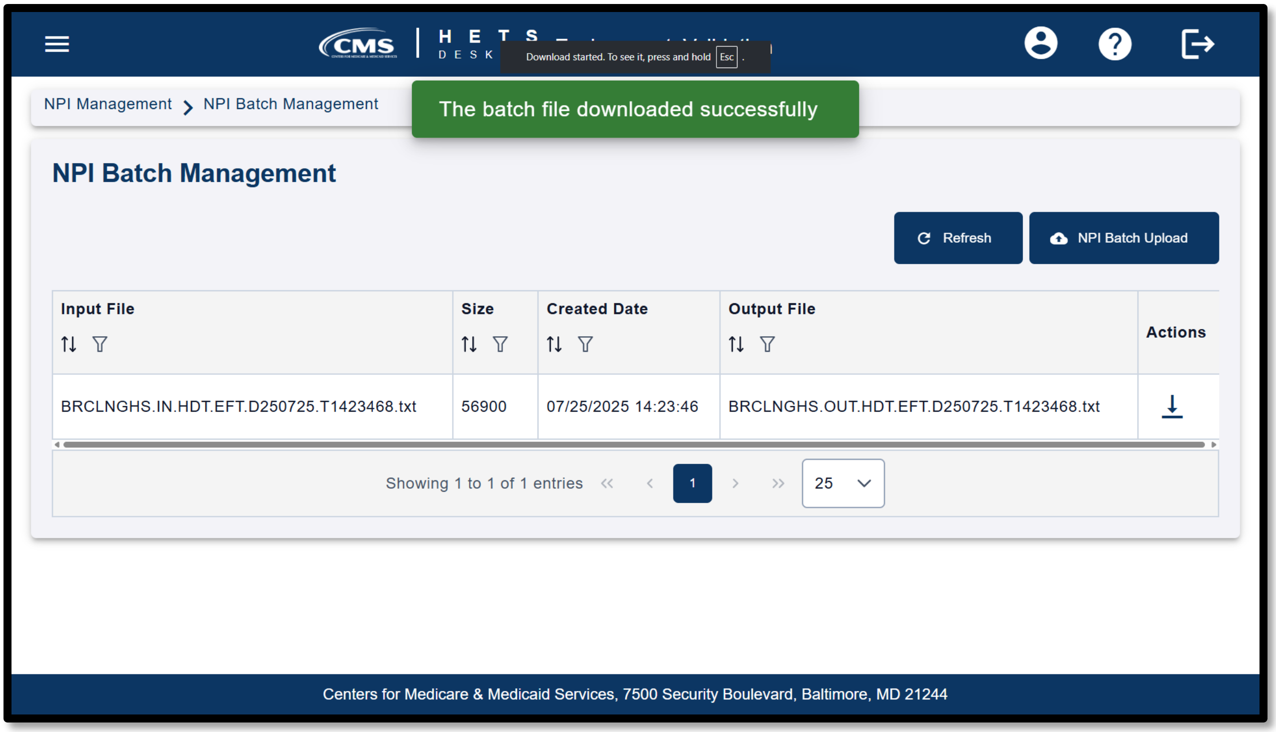
Input File	Size	Created Date	Output File	Actions
BRCLNGHS.IN.HDT.EFT.D250725.T1423468.txt	56900	07/25/2025 14:23:46	BRCLNGHS.OUT.HDT.EFT.D250725.T1423468.txt	⤓

Figure 44: Batch File in Progress

1.9.2.2 Downloading Output File

To download a results file, follow these steps:

1. Select the appropriate Output File that you would like to review from the Batch File in Progress page shown above. Select the ‘Download File’ icon on the row of the appropriate file.
2. “The batch file download successfully” will display on the screen as illustrated in *Figure 45: Batch File Downloaded Successfully*. The file will be downloaded to your machine’s default download location. The file will be saved as the default file name of the HDT Batch output file.


HETS DESK
Download started. To see it, press and hold Esc .
NPI Management > NPI Batch Management
Refresh
NPI Batch Upload
Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

The batch file downloaded successfully

NPI Batch Management

Input File	Size	Created Date	Output File	Actions
BRCLNGHS.IN.HDT.EFT.D250725.T1423468.txt	56900	07/25/2025 14:23:46	BRCLNGHS.OUT.HDT.EFT.D250725.T1423468.txt	⤓

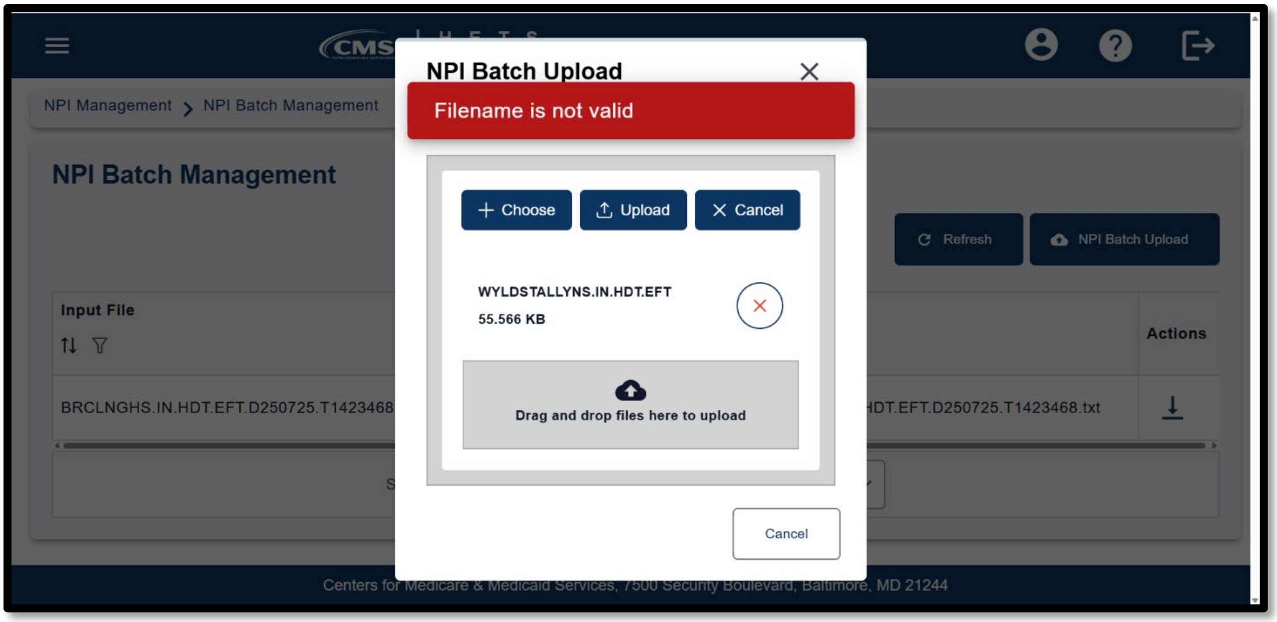
Showing 1 to 1 of 1 entries 1 25

Figure 45: Batch File Downloaded Successfully

1.9.3 Invalid File Name Format Error

If an HDT user from a Clearinghouse attempts to upload a batch input file that does not meet the required naming convention specified in the

Input File section, HDT will display an error message of “Filename is not valid” on screen, illustrated in *Figure 46: Invalid File Name Format*.


NPI Management > NPI Batch Management
NPI Batch Management
Refresh
NPI Batch Upload
Input File
Actions
BRCLNGHS.IN.HDT.EFT.D250725.T1423468
DT.EFT.D250725.T1423468.txt
+ Choose
Upload
× Cancel
Drag and drop files here to upload
Cancel
Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, MD 21244

NPI Batch Upload

Filename is not valid

WYLDSTALLYNS.IN.HDT.EFT
55.566 KB

Figure 46: Invalid File Name Format

1.10 HDT Troubleshooting & Support Information

1.10.1 Troubleshooting

HDT application hours of operation are determined by CMS policy, support, hardware availability, and availability of required interfaces.

The HDT database will be available during the following time periods:

- Monday: 6 am - 11:59 pm ET
- Tuesday: 6 am - 11:59 pm ET
- Wednesday: 6 am - 11:59 pm ET
- Thursday: 6 am - 11:59 pm ET
- Friday: 6 am - 11:59 pm ET
- Saturday: 12 am - 11:59 pm ET
- Sunday: 12 am - 6:59 pm, 9 pm – 11:59 pm ET

Users may be able to log in to the HDT application outside these days/times, but the NPI Management functionality will be disabled. If users upload a file to the EFT system using the NPI Batch Management functionality, the batch input file will not be processed until the database becomes available.

If users submit a batch file that does not complete processing before the system becomes unavailable, the batch output file will include an error message that the file could not be processed. The Submitter will need to upload the file again when the HDT database is available.

Scheduled maintenance outages are communicated to users via email. In addition, MCARE Help Desk support is available Monday through Friday, 7:00 am – 7:00 pm ET.

1.10.2 Support Information

If problems or questions arise while accessing the HDT application, contact the MCARE Help Desk at 1-866-324-7315 or MCARE@cms.hhs.gov, Monday through Friday, from 7:00 am to 7:00 pm ET.

Note: MCARE email is monitored during regular business hours. Emails are typically answered within one business day.

1.11 HDT Error Messages

1.11.1 Access and Behavior Error Messages

HDT returns a variety of unique errors related to User access or behavior issues. Each error displays a specific recommendation on screen. Users should follow the on-screen recommendations. When directed to do so, users should note the error message they receive and then contact the MCARE Help Desk for assistance. For contact information for the MCARE Help Desk, refer to HDT Troubleshooting & Support Information.

1.11.2 Batch File Error Messages

Table 5: Batch File Error Messages identifies the error messages that will be returned in the output file when the input file cannot be processed for the indicated reasons.

Table 5: Batch File Error Messages

Error Message	Condition(s)
Failed to validate file. The file is empty.	The batch file contains no data.
Line #${lineNumber}: Each line must have 3 values: Submitter ID, NPI, and Action	A line in the batch file does not include the three requisite elements.
Line #${lineNumber}: Action must be either A, Q, or T	A line in the batch file does not include one of the three requisite action code values.
Line #${lineNumber}: Submitter ID length must not exceed 10	A line in the batch file contains a value in the Submitter ID field that exceeds 10 characters.
Line #${lineNumber}: NPI length must be 10. Legacy ID/Source ID is no longer a valid request	A line in the batch file contains a value in the NPI field that is not 10 characters.
Line #${lineNumber}: File could not be processed further.	A line in the batch file cannot be processed.
Line #${lineNumber}: Submitter ID is invalid. File could not be processed further.	The Submitter ID within the file is: • Not found, • Not associated with the Submitter ID in the file name, • Suspended, or • Terminated.
A file has already been submitted by Submitter ID ${Submitter ID}. A Submitter can only submit one file in a day.	A Submitter uploads more than one file during a single calendar day using the NPI Batch Management function in HDT.

1.12 Special Considerations

1.12.1 Data Size Limits

The HDT NPI Batch Management input file must be less than 10MB.

1.12.2 Daily Batch File Submission

Clearinghouse Submitters are limited to uploading one batch file per day. If a Clearinghouse Submitter attempts to upload more than one file during a single calendar day, an error message is returned in the batch output file.

Appendix A: Revision History

Table 6: Record of Changes

Version Number	Date	Description of Change
2.0	9/4/2025	Document TW review, finalization, and baselining. Accepted prior edits.
2.0	08/22/2025	The document was updated to remove duplicative information already contained within CMS IDM User Guides. Several sections were removed; users should refer to the IDM user documentation for tasks or processes that are not HDT-specific. Updated Section 2 to include links to CMS IDM documentation for both general use as well as Remote Identity Proofing. Sections 7 - 9 were updated to reflect the revised HDT layout and functionality following the HDT 2025 Redesign. Section 12 updated to note that HDT Batch input files must be less than 10MB. Removed Appendices B & C.
1.9	08/09/2024	Updated the following: Updated Experian support phone number from 866-578-5409 to a new number of 833-203-6550. This change is effective in August 2024.
1.8	04/24/2024	Updated the following: Removed all references to IDM providing HDT users the option to select “Do not challenge me…” during the IDM sign-in/MFA process. This option is no longer available in IDM. Updated all related screenshots.
1.7	11/16/2023	Updated the following: Removed Contract Number and Document Number. Section 1.3 to provide additional details about IDM security policy measures to deactivate and remove unused accounts.
1.6	08/18/2023	Updated the following: Updated Contract Number. Section 5.3 to include YubiKey as an MFA factor. New User Registration Form in section 6. Manage MFA and Recovery Devices throughout. Section 13.3 to remove the Remote Identity Proofing questions and to update the identity proofing steps.

Version Number	Date	Description of Change
1.5	03/10/2023	Updated document to reflect updated CMS password policy changes effective in April 2023. Changes include: Section 3, Table 1 updated links Section 5.2, updated to reflect CMS password policy changes including a list of special characters that may be used if the User chooses to include a special character in their 15 character (or more) IDM password Section 7, updated screenshots to reflect changes to CMS password policy
1.4	04/23/2022	Updated Section 14.1 to note that the full HDT URL address is https://HDT.hetsp-haa.cms.gov/HDT/.
1.3	04/8/2022	Updated Section 14.1 to note that the HDT URL has changed from https://cmshdt.cms.gov/HDT/ to https://HDT.hetsp-haa.cms.gov.
1.2	12/16/2021	Updated Section 4.1 to remove Internet Explorer (IE) from the list of supported internet browsers. Effective January 9th, 2022, CMS Enterprise Portal Services (EPS) no longer supports the IE browser. The EPS landing page will no longer load or be accessible for IE users in the Production environment after January 9, 2022.
1.1	04/23/2021	Updated Section 5.1 to reflect revisions to the HDT policy regarding allowable characters in the IDM User ID or the user’s first and/or last name.
1.0	01/14/2021	Initial draft.