Centers for Medicare & Medicaid Services

HETS Desktop (HDT) User Guide

Version 3.0

12/18/2025

Table of Contents

List of Figures

List of Tables

1.1 Introduction

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

HDT leverages the Centers for Medicare and Medicaid Services (CMS) enterprise Identity Management (IDM) system for user access and verification. Effective December 2025, new HDT users may choose to authenticate using a validated (new or existing) Login.gov account instead of CMS's IDM. HDT users whose access was established via IDM before December 2025 will continue to utilize their IDM credentials to access HDT until advised otherwise. Regardless of how the user authenticates, the processes for obtaining HDT access and using HDT are identical for both IDM and Login.gov credentials.

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 obtain HDT access in IDM after authenticating through either IDM or Login.gov.
- 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 they send only active, valid Fee-for-Service (FFS) Medicare National Provider Identifier (NPI) numbers to the HETS 270/271 application.

Currently, HETS Submitters must utilize HDT 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.

CMS also requests that Medicare Providers and Suppliers enroll and attest to a known trading relationship with a HETS vendor or Clearinghouse via the Provider or Supplier MAC. In Spring 2026, we'll transition to a new HETS trading partner management system. HETS will reject NPI eligibility requests without enrollment. HETS vendor or Clearinghouse Submitters must inform customers of this requirement to ensure they maintain HETS access. Vendors or Clearinghouses can track the enrollment status of your customers' NPI using HDT.

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

This user guide provides step-by-step instructions for performing the following tasks (based on access privileges) to obtain HDT access:

- How to request HDT access via IDM after authenticating using IDM or Login.gov credentials

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 enrollments (or '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 enable business partners to request and obtain a single User ID 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 an enhanced user experience on desktop and laptop computers, as well as on tablet and smartphone devices.

The IDM security policy includes processes to disable inactive IDM user accounts that have been inactive for 60 days. These users must update their IDM password during reactivation. IDM users who remain inactive for two years will have their accounts removed. These users are notified by email before their accounts are 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 Login.gov Overview

Login.gov was launched in 2017 in response to the Federal Cybersecurity Requirements statutory mandate (6 USC § 1523 — Federal cybersecurity requirements, part (b)(1)(D)) that instructed agencies to "implement a single sign-on trusted identity platform for individuals accessing each public website of the agency that requires user authentication as developed by the Administrator of General Services " and "implement identity management…including multi-factor authentication."

Initially developed as a combined effort by technologists at the General Services Administration (18F) and the U.S. Digital Service, the team included engineers, designers, user experience experts, and product managers with experience in similar authentication systems in the government and in the private sector. Today, the Login.gov program is operated as a standalone division within the GSA's Technology Transformation Services.

Login.gov has continued to develop to meet changing standards and agency needs. Important milestones include the launch of identity verification in Fall 2018, reaching one million proofed accounts in August 2022, and the launch of a NIST IAL2-compliant offering in September 2024.

Note that Login.gov accounts can be used across a variety of federal agencies and applications. Additional information about Login.gov is available in *Referenced Documents.*

1.1.5 HDT Application Overview

Users access the HDT application after authenticating their identity using IDM or Login.gov. Approved IDM and Login.gov users must add the HDT role to their profile via IDM during the application process, then obtain CMS approval before HDT access is granted.

Submitters use the HDT application to:

- Register their HETS 270/271 Provider/Supplier customers with CMS to establish an NPI/Submitter relationship (required through Spring 2026)
- Maintain a list of all NPIs that their organization will be sending to the HETS 270/271 application (required through Spring 2026)
- View a list of associated NPIs and their HETS trading status
- Query the status for one or more NPIs via NPI management
- Vendor or Clearinghouse Submitters can download a list of all active Medicare Provider/Providers and Suppliers who created attestations

HDT 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 invalid by Medicare, it will also be invalid in HDT and will be prohibited from receiving PHI via 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, HDT validates that there is a known Submitter/Provider relationship between the HETS 270/271 Submitter and the FFS Medicare Provider or Supplier.

HDT allows for both manual and batch NPI management processes. The manual NPI management options allow vendor or 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 vendor or Clearinghouse Submitters to query, add, or terminate their relationships for multiple NPIs at once. The NPIs must be submitted in a flat text file that can be uploaded via HDT. HDT vendor or Clearinghouse Submitter Users can upload batch files and then receive response files back via HDT. 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.

HDT is integrated with the HETS 270/271 application. The NPIs submitted with 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.

CMS also requests that Medicare Providers and Suppliers enroll and attest to a known trading relationship with a HETS vendor or a Clearinghouse through their Provider or Supplier MAC. In Spring 2026, we'll transition to a new HETS trading partner management system. HETS will reject NPI eligibility requests without enrollment. HETS vendor or Clearinghouse Submitters must inform the customers of this requirement to ensure they maintain HETS access. Vendors or Clearinghouses can track the enrollment status of your customers' NPI using HDT.

- HETS vendor or 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-vendor or 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 documents related to Remote Identity Proofing (RIDP). All HDT users who authenticate via IDM must complete RIDP.

The Login.gov Help Center provides comprehensive information on creating an account, verifying your identity, signing in, and managing your Login.gov account. All HDT users who authenticate via Login.gov must verify their identity via Login.gov.

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.

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
Login - Need to sign in to HDT?	Navigate to https://HDT.hetsp-haa.cms.gov/HDT/ or see Section Log In to the HDT Application
Access - Need to add an HDT role to an existing account?	See Section *How to Request HDT Access*
Access -- Need to manage your HDT role in IDM after authenticating?	Refer to Sections 6-10 of the CMS IDM User Guide
HDT - Need to create a new NPI relationship?	See Section *NPI Management*
HDT - Need to submit a Batch file?	See Section *NPI Batch Management*
HDT - Need to download a list of your customers' active attestations?	See Section *Download Active Provider Attestation List*
HDT - Getting an error message?	See Section *HDT Error Messages*
IDM - Need to sign in to IDM?	Navigate to https://home.idm.cms.gov/ or refer to Section 5 of the CMS IDM User Guide
IDM - Need to create an entirely new IDM account?	Refer to Section 4 of the CMS IDM User Guide
IDM - Need to add a Multi-factor Authentication (MFA) device to your IDM account?	Refer to Section 11 of the CMS IDM User Guide

Questions	Answers
IDM – Need to reset or unlock your account? Need to change your password?	Refer to Section 10 of the CMS IDM User Guide
IDM - Need help with Remote Identity Proofing?	Refer to IDM's RIDP resources
Login.gov - Need to sign in to your Login.gov account?	Navigate to https://secure.login.gov/
Login.gov - Need to create an entirely new Login.gov account?	Refer to https://login.gov/help/create-account/overview/
Login.gov - Need to add a Multi-factor Authentication (MFA) device to your account?	Refer to https://login.gov/help/create-account/authentication-methods/security-key/
Login.gov – Trouble signing in? Need to change your password?	Refer to https://login.gov/help/trouble-signing-in/overview/
Login.gov - Need help verifying your identity?	Refer to https://login.gov/help/verify-your-identity/overview/

1.4 Prepare to Access the HDT Application

Users who access HDT after authenticating via IDM or Login.gov with a desktop or laptop computer may need to perform software updates or configure web browser settings and privacy settings. Users who access HDT after authenticating via IDM or Login.gov 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, IDM, and Login.gov were tested for compatibility with current versions of the following modern web browsers:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Safari

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

1.4.2 Verify Screen Resolution

The HDT application, IDM, and Login.gov are optimally viewed on a display resolution of 1366 × 768. All images displayed on modern computing devices are composed of a matrix of thousands of tiny dots, called pixels. This matrix is expressed as width × height (for example, 1366 pixels wide × 768 pixels high, or 1366 × 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 × 768. The HDT application, IDM, and Login.gov 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 of 1366 × 768 pixels or higher. Users of older devices or operating systems may need to change their display resolution settings if the current setting does not display the page 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 uses similar page components, the user's browser must be configured to attempt to locate and retrieve a fresh instance of the HDT page and its data.

HDT users should enable JavaScript and adjust any zoom settings to ensure they are not viewing the screen at an angle that is too wide.

HDT users should disable Compatibility View in their web browsers to ensure HDT pages display correctly.

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 user authenticates via IDM or Login.gov to verify their account credentials. In addition to standard IDM or Login.gov 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 the CMS password policy. Both IDM and Login.gov User IDs that are used to access HDT must conform to the following guidelines:

- Only personnel from the HETS vendor or 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 or Login.gov User ID that has 32 characters or fewer to utilize the HDT application.
- The HDT application allows the IDM or Login.gov User ID and the 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 or Login.gov 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. IDM or Login.gov 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

New HDT users can request access to the application (and an appropriate role) by using the ***Role Request*** button.

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

While HDT now supports user authentication via either IDM or Login.gov, once the user is logged in, requesting new HDT access is handled via IDM. Login.gov will automatically forward the user to IDM as needed for this process.

New HDT role requests consist of the following steps:

1. User navigates to https://HDT.hetsp-haa.cms.gov/HDT/
2. The user signs in via their existing IDM or Login.gov account.

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

If needed, the user completes the identity verification process. [1]

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. [2, 3]

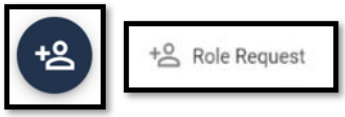

Figure 2: Role Request Button and Role Request Taskbar Option

2. Use the Select Application drop-down menu to select an application. [4]
3. Enter “HDT,” and you will have an option to select the HDT application. [5]

---

[1] IDM or Login.gov users that have previously verified their identity will not be required to complete this process again. IDM user accounts verify their identity via Remote Identity Proofing process. Login.gov user accounts verify their identity via a different process.

[2] 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.

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

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

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

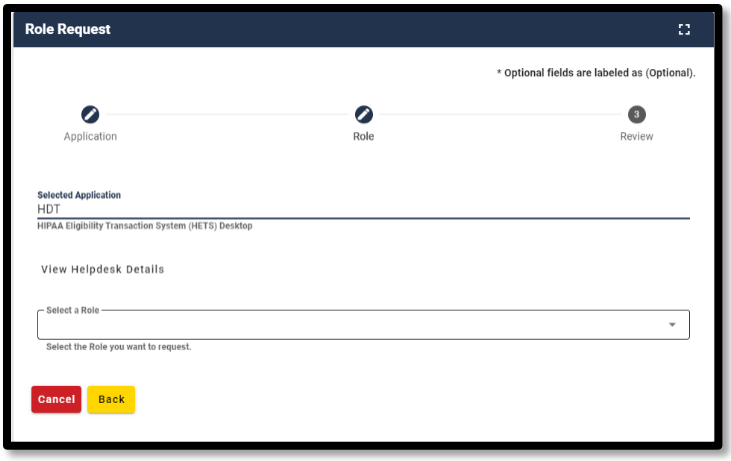

Figure 3: Role Request that Requires Application and Role

4. (Optional) Select the ***View Helpdesk Details*** button to display the Application Helpdesk Details UI. [6]

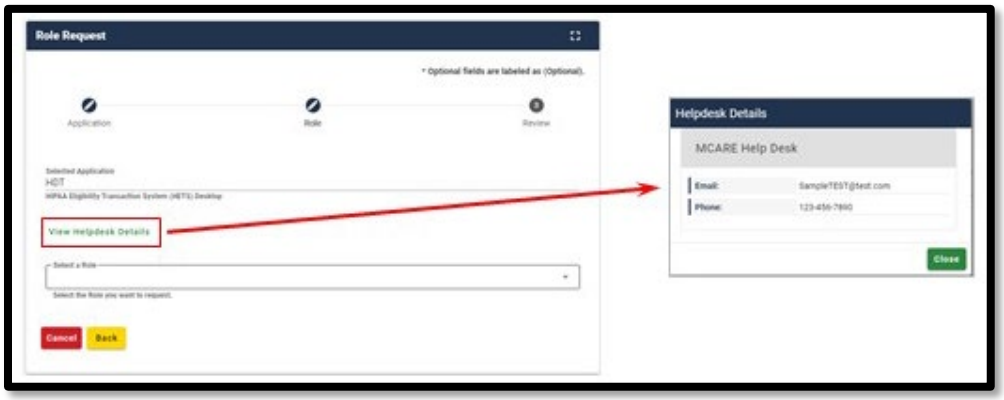

Figure 4: Role Request Helpdesk Details (Optional Step)

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.

[6] 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.

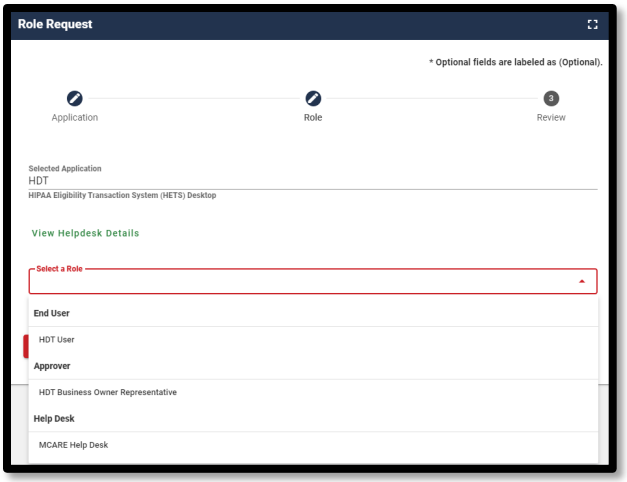

Figure 5: Role Request Specifying HDT Role

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*.

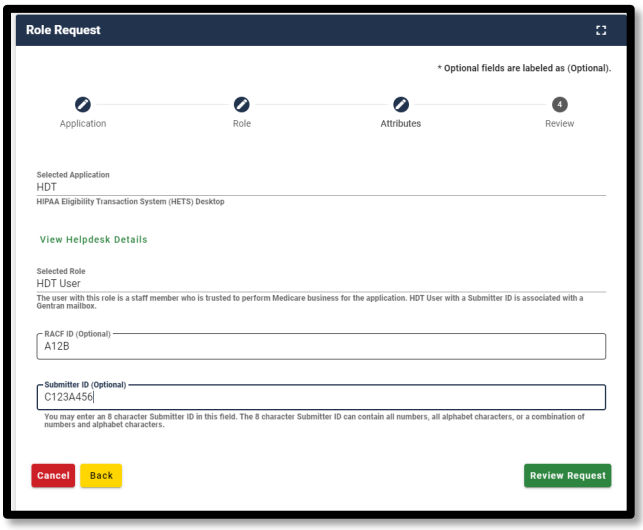

Figure 6: Role Request Specifying Additional Details

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.

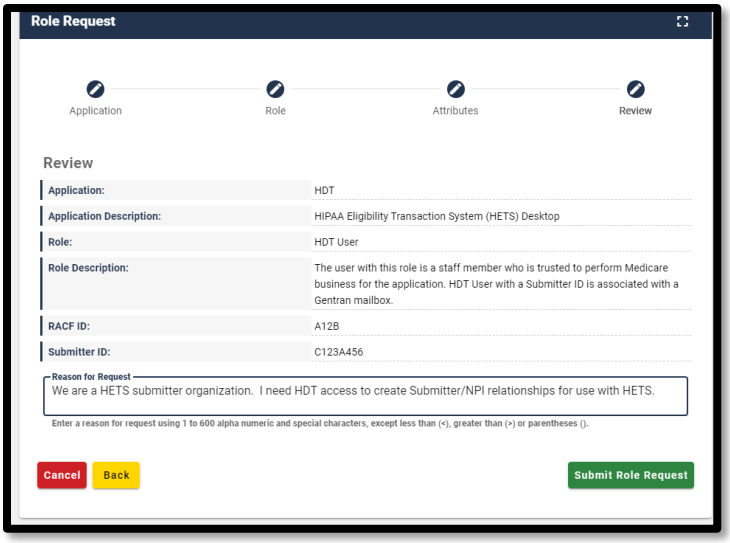

Figure 7: Role Request Ready for Submission

9. Select the ***Submit Role Request*** button. [7, 8]

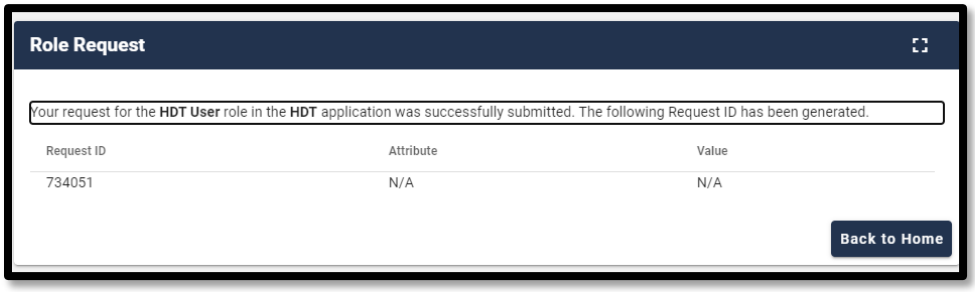

Figure 8: Successful Role Request Message

10. The Role Request UI displays a Request ID and a message that informs the user that the request was successfully submitted. [9]
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.

---

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

8 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.

9 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 shows 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 shows 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 being taken by an approver. It also shows where the user can obtain assistance if they have questions.

1.7 Using the HDT Application

The following subsections provide detailed, step-by-step instructions for using the HDT application's features.

1.7.1 Log In to the HDT Application

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

Enter the HETS Applications Portal in a web browser.

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 HDT login screen displays as illustrated in *Figure 10: HDT Sign In Window.*

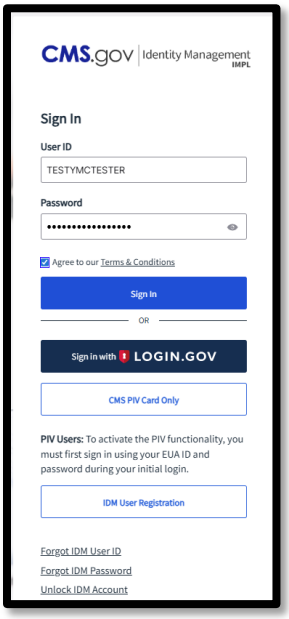

Figure 10: HDT Sign In Window

If you have an IDM user account, follow the instructions in 1.7.1.1.

If you have a Login.gov user account, follow the instructions in Section 1.7.1.2.

1.7.1.1 IDM User Log-in Instructions

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

   The HDT login screen displays as illustrated in *Figure 11: HDT Sign In Window.*

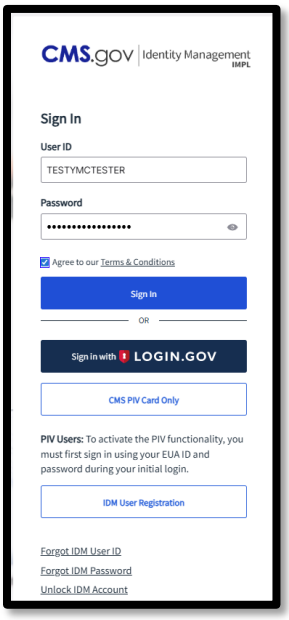

Figure 11: HDT Sign In Window

2. Type the User ID into the User ID field.
3. Type the Password into the Password field.

   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 12: An Example Sign in Error: Agree to Terms & Conditions.*

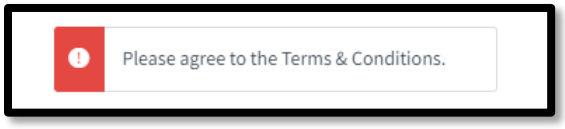

Figure 12: An Example Sign in Error: Agree to Terms & Conditions

4. Select the **Sign In** button. The MFA One-time Password (OTP) Request window appears. Check the box to acknowledge agreement with the Terms & Conditions.

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.

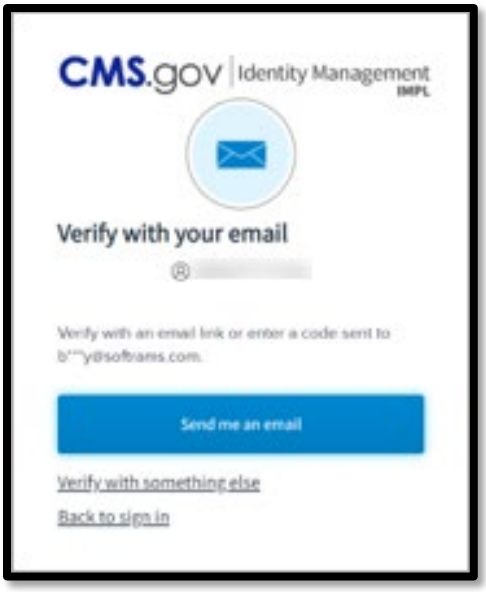

Figure 13: MFA OTP Request Window

5. Select the ***Send me an email*** 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 email, voice message, text message, or push notification, depending on the user's MFA device choice.

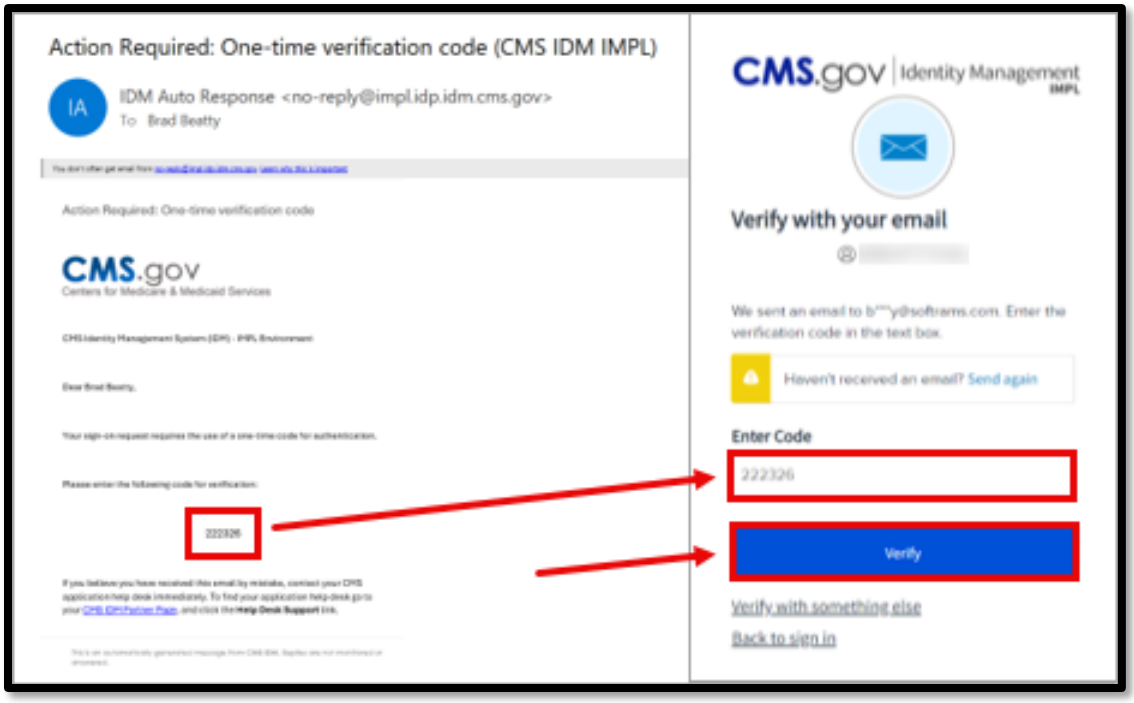

Figure 14: Sample MFA OTP Email and the MFA Verification Window

6. The MFA device returns an OTP. Enter the OTP into the 'Enter Code' field. If the MFA device supports push notifications, no code is 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 *Error! Reference source not found.*.
- The user may select the ***Send again*** link to request another OTP if the original OTP request failed.

7. 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 18: 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.

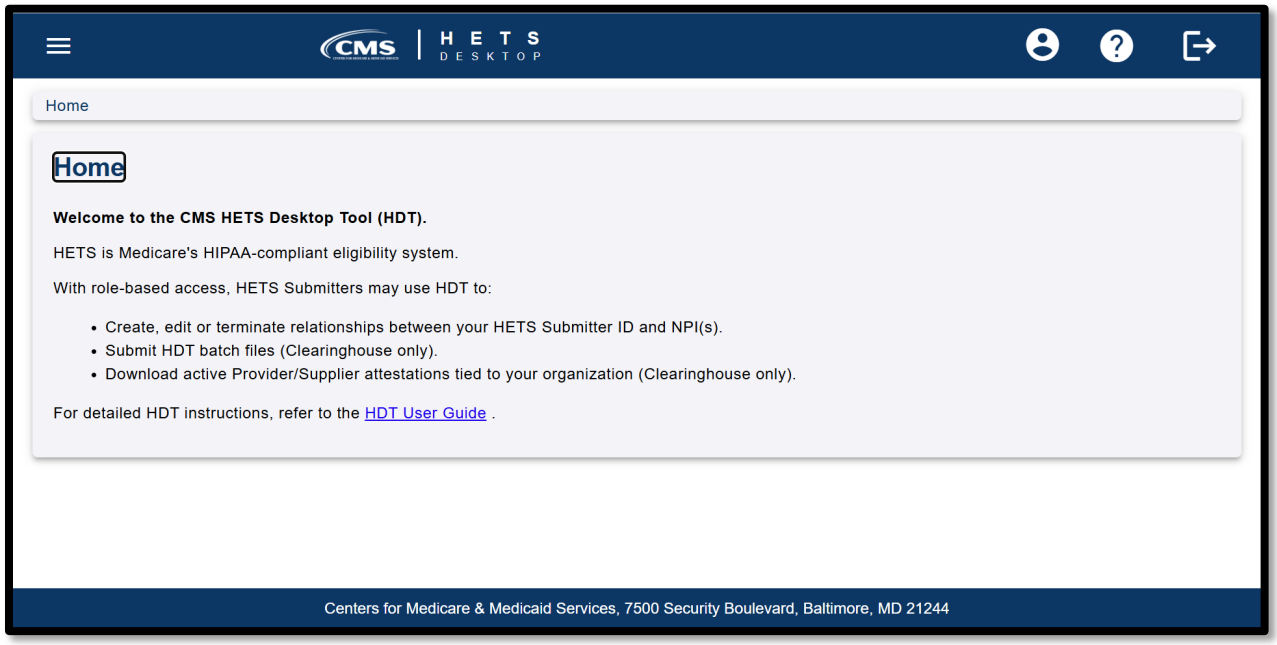

Figure 15: HETS Desktop Home Screen

1.7.1.2 Login.gov User Log-in Instructions

Enter the CMS Applications Portal in a web browser.

The HDT login screen displays as illustrated in *Figure 16: HDT Sign In Window.*

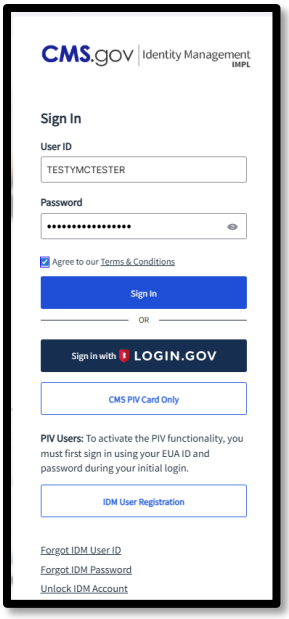

Figure 16: HDT Sign In Window

1. Instead of entering your User ID and Password, select the ***Sign in with LOGIN.GOV*** button. You will be forwarded to Login.gov, as illustrated in *Figure 17: Login.gov Authentication Window*.

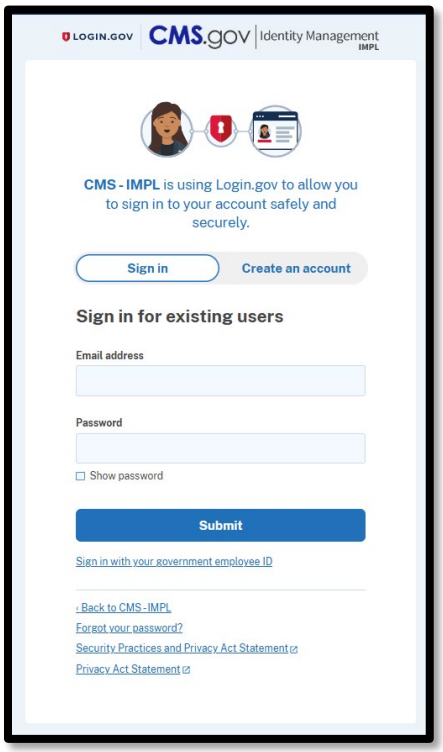

Figure 17: Login.gov Authentication Window

2. Enter your registered Email address and Login.gov Password into the appropriate fields. Check the ***Show password*** box, and select the ***Submit*** button.
3. Authenticate using one of the Login.gov options you set up, such as:

   a) Scanning your face or fingerprint
   b) Entering a one-time code from your authentication application
   c) Using your security key
   d) Entering a one-time code that you receive by text or by phone call
   e) Entering a backup code
   f) Using your federal government employee or military ID (PIV or CAC)

4. You will then be taken to the HETS Desktop Home Screen as illustrated in *Figure 18: HETS Desktop Home Screen*.

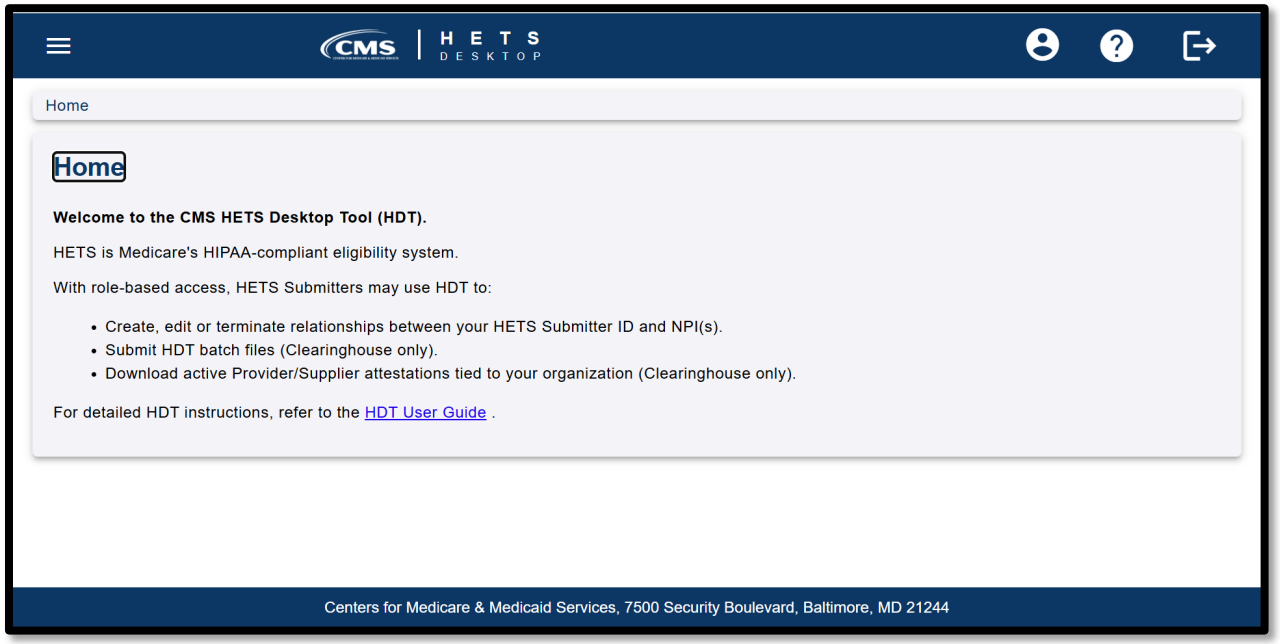

Figure 18: HETS Desktop Home Screen

1.7.2 HETS Desktop Home Screen

When users log in to the HDT application, the HETS Desktop home screen displays as illustrated in *Figure 18: 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 increases display settings, some items that were previously consolidated into menus may expand into 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 18: 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).

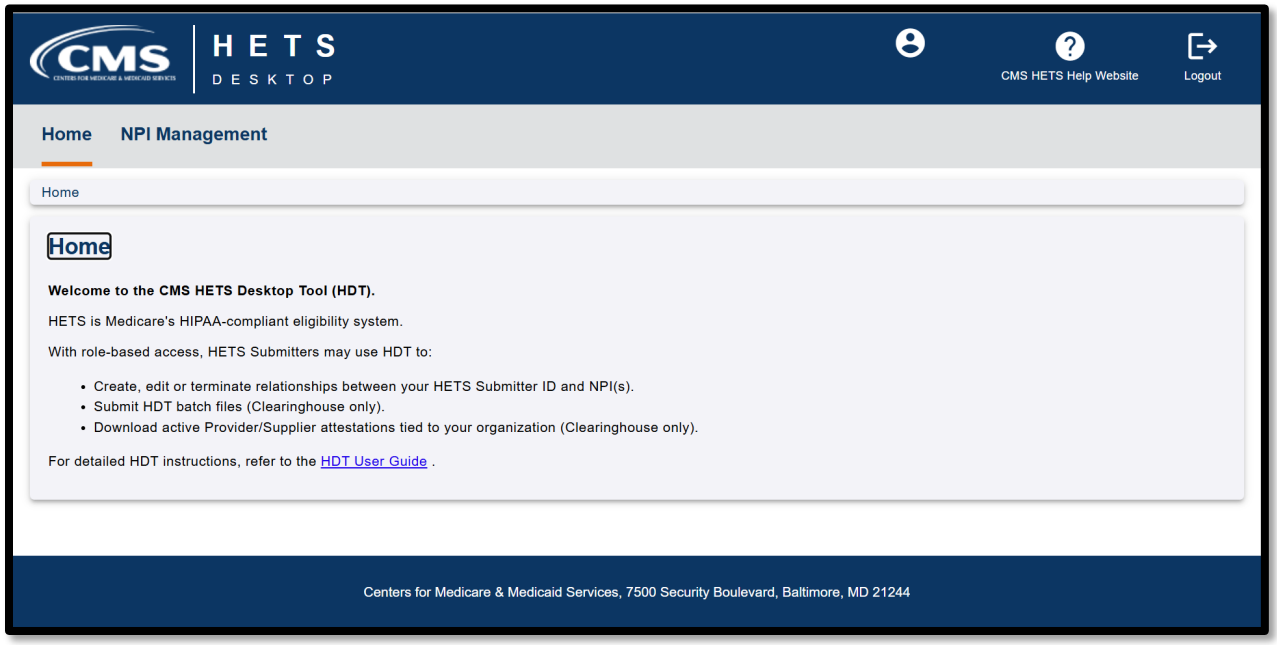

Figure 19: HETS Desktop Home Screen Expanded View

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 vendor, 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 vendor or 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 vendor or Clearinghouse Submitters only. Vendor or 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 28: IDM System Sign In Page*.

1.7.3 Application Layout

The application layout in the Site Map, as illustrated in *Figure 27: 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 vendor or 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 20: Menu Icon

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

Figure 21: 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 22: CMS HETS Help Website Icon

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

Figure 23: View Icon

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

Figure 24: Terminate Icon

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

Figure 25: Download File Icon

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

Figure 26: Logout Icon

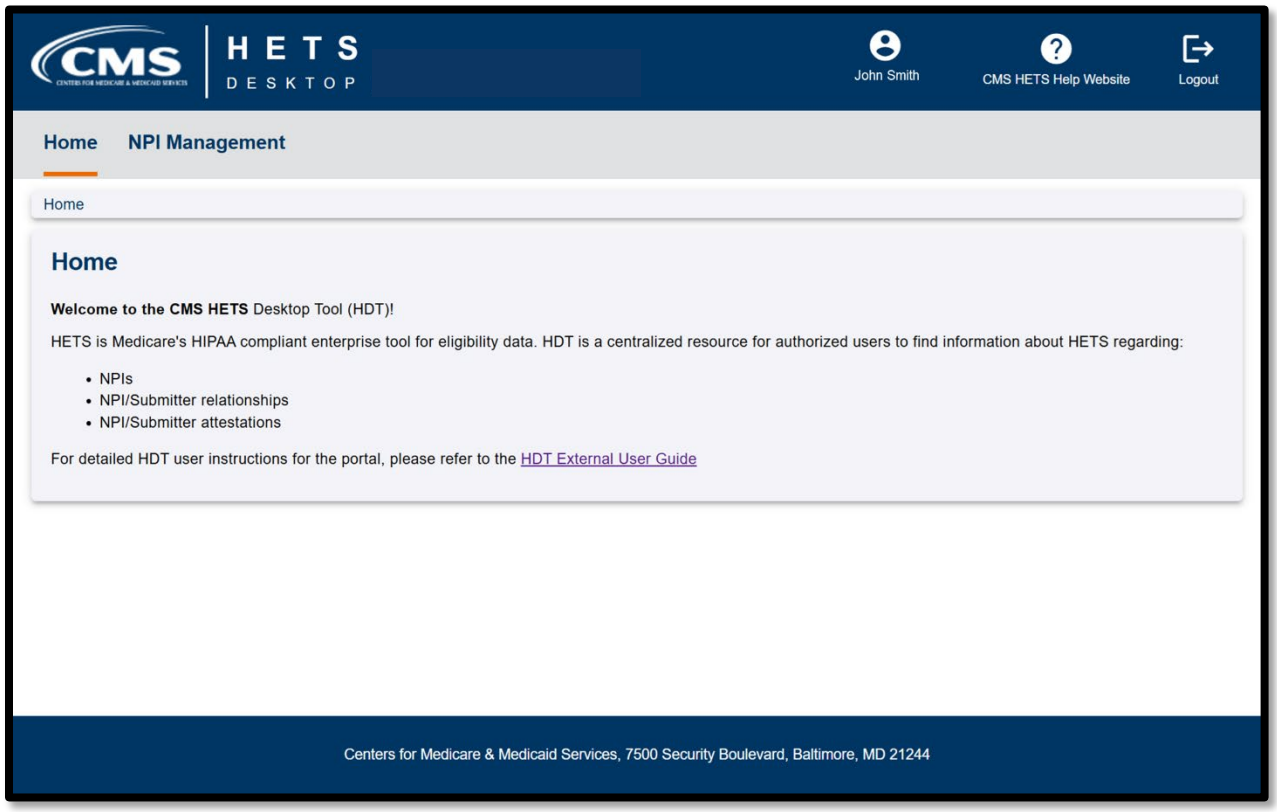

Figure 27: HDT Application Site Map

1.7.4 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 28: IDM System Sign In* **.**

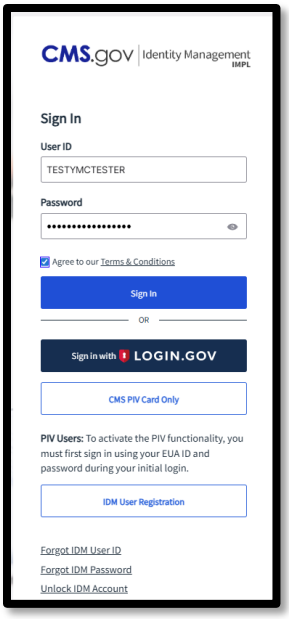

Figure 28: IDM System Sign In Page

1.8 NPI Management

NPI Management allows vendor or Clearinghouse and Direct Provider Submitters to query, add, or terminate relationships with NPI numbers. Direct Provider Submitters may perform this task for only one NPI at a time using the NPI Management List feature. HETS vendor or Clearinghouse Submitters can use the NPI Batch Management feature to manage multiple NPIs at once. HETS vendor or 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 29: HDT NPI Management Displaying Both Regular and Batch Options*.

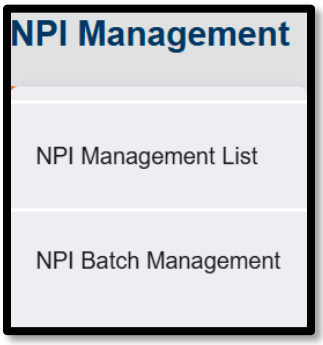

Figure 29: HDT NPI Management Displaying Both Regular and Batch Options

1.8.1 NPI Management List

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

Note: Data varies by 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 30: NPI Management List Page*.

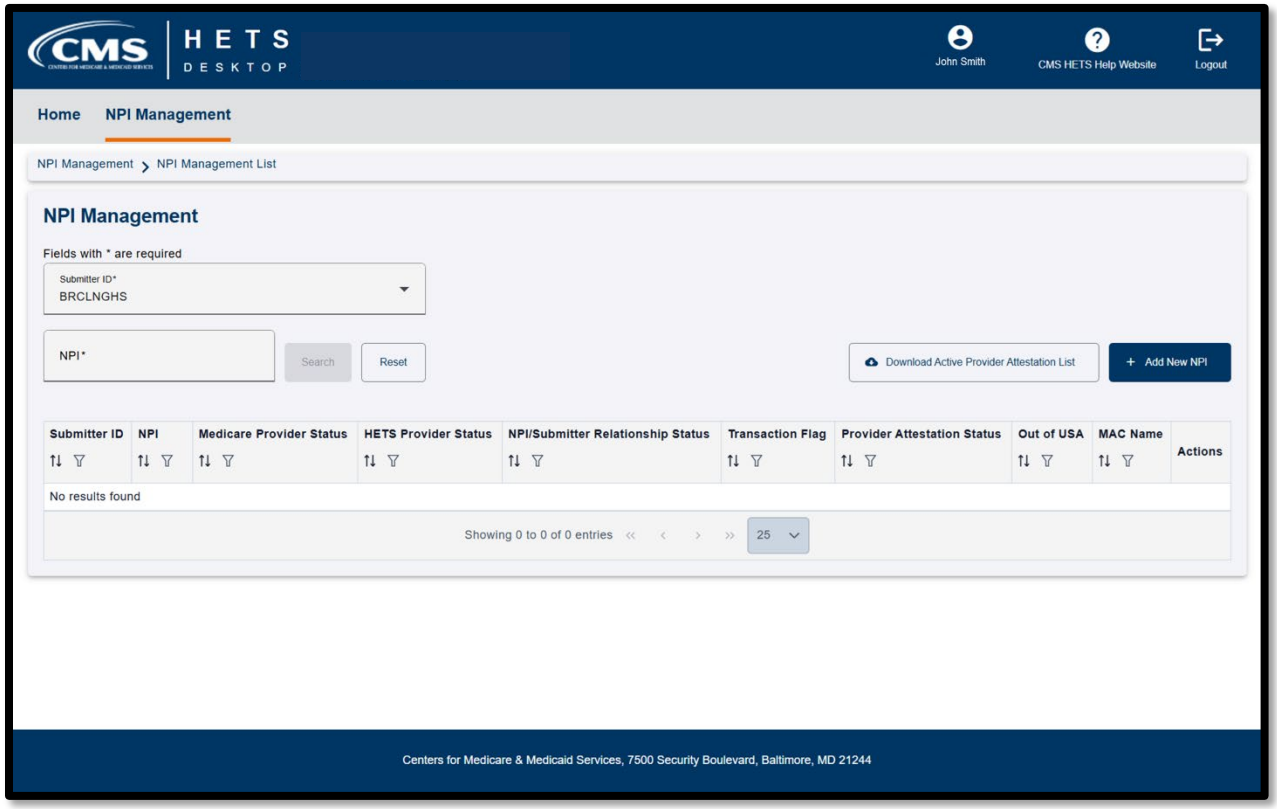

Figure 30: NPI Management List Page

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 31: HDT NPI Management Screen – Search Results.*

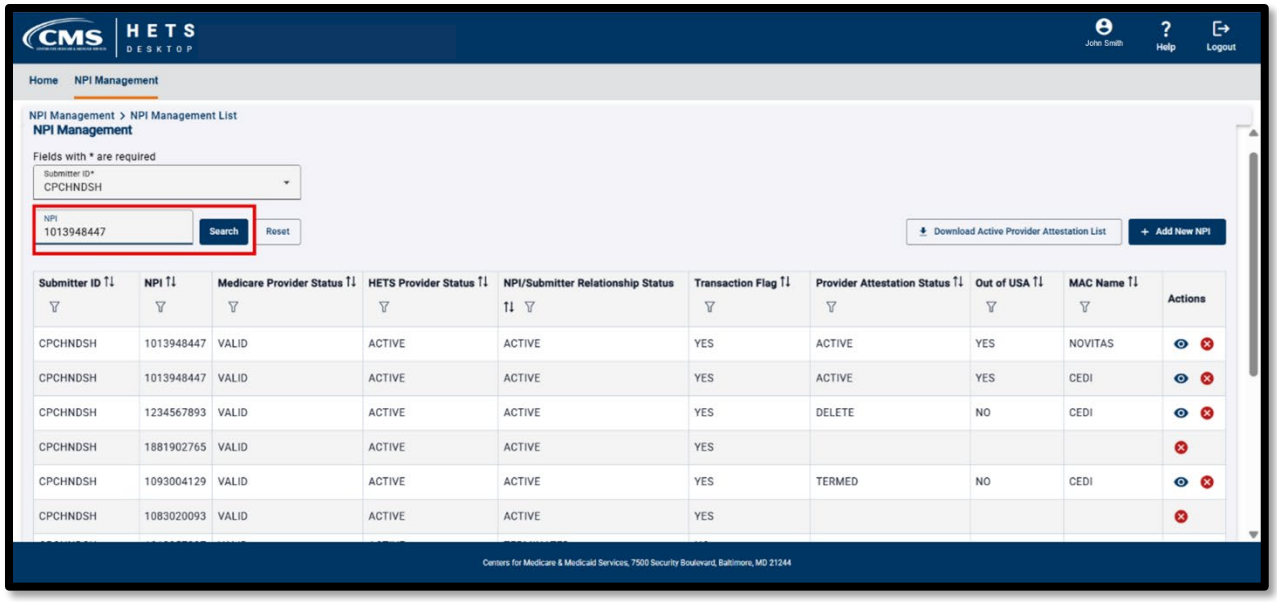

Figure 31: HDT NPI Management Screen – Search Results

4. Results for requested actions are displayed in an NPI Results table, as illustrated in *Figure 32: HDT NPI Management Screen – NPI Entered Search Results*.

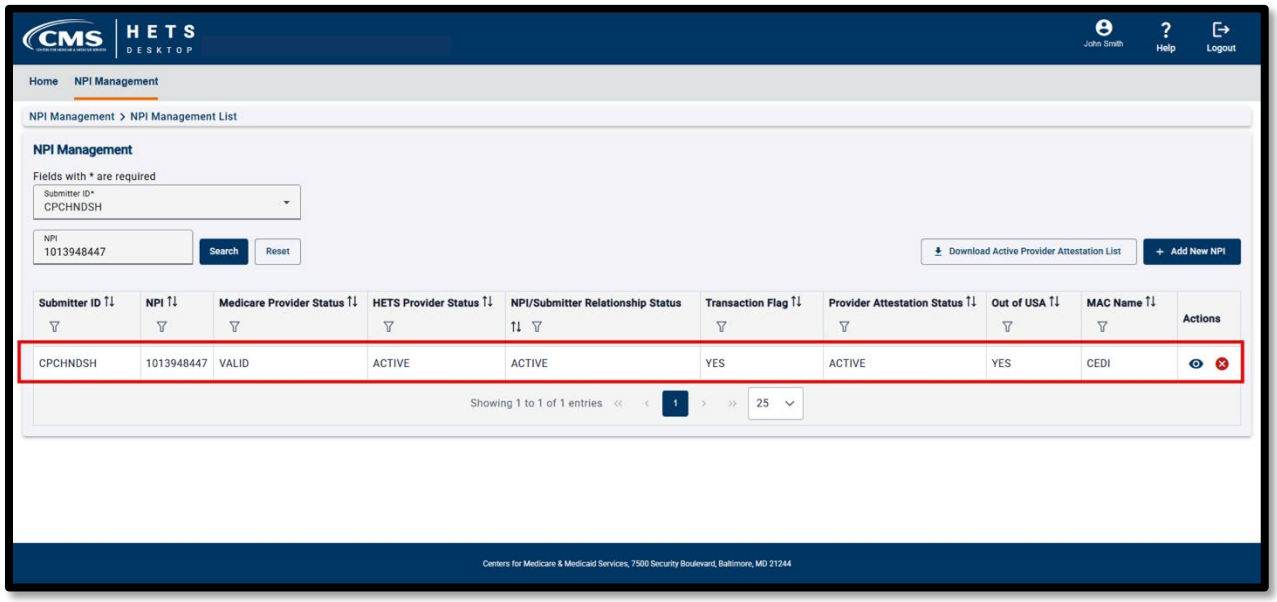

Figure 32: HDT NPI Management Screen – NPI Entered Search Results

Note: The table displays 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.
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 vendor or 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 vendor or 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 MAC name 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 vendor or 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 'Yes', the NPI can be 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 vendor or Clearinghouse Submitter users. Direct Provider Submitter users will not have access to this data.

5. If a vendor or 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 33: HDT NPI Management Screen – Attestation View*.

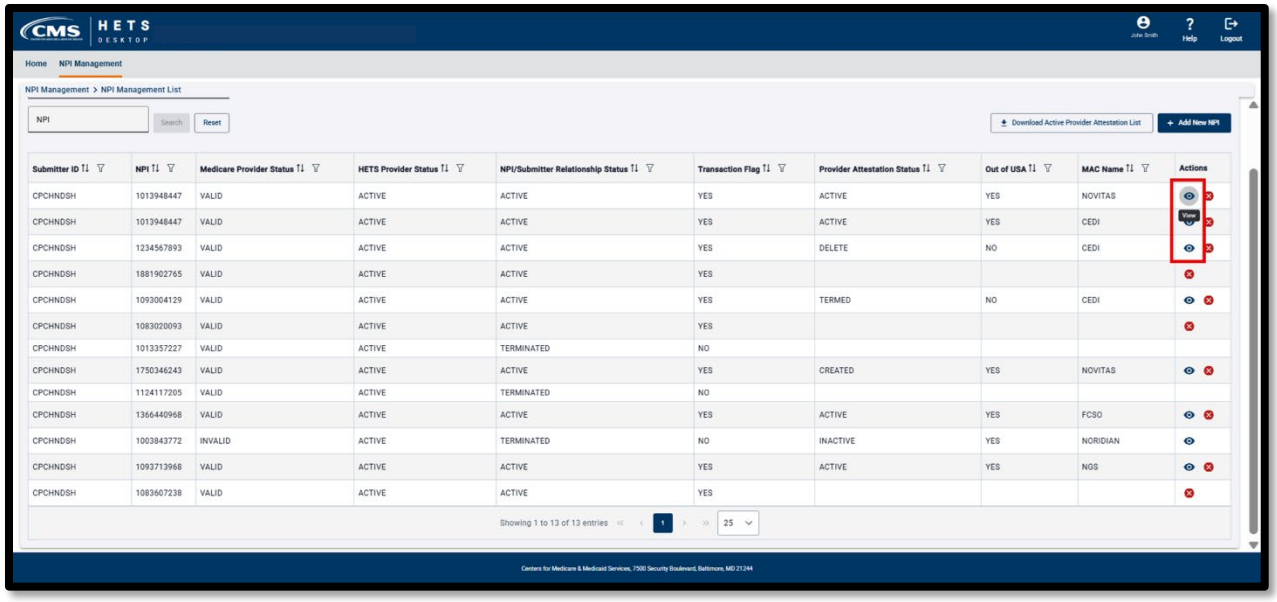

Figure 33: HDT NPI Management Screen – Attestation View

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 34: HDT NPI Management Screen – Attestation Detail View*.

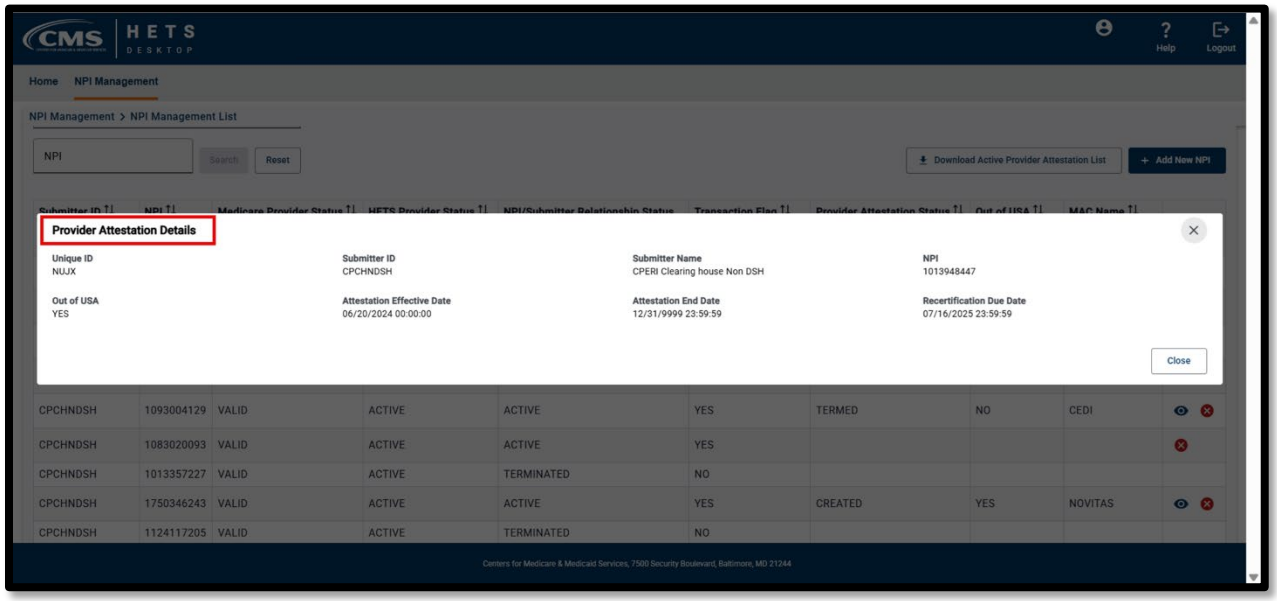

Figure 34: HDT NPI Management Screen – Attestation Detail View

Note: The HETS vendor or 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 35: HDT NPI Management Screen – Add*.

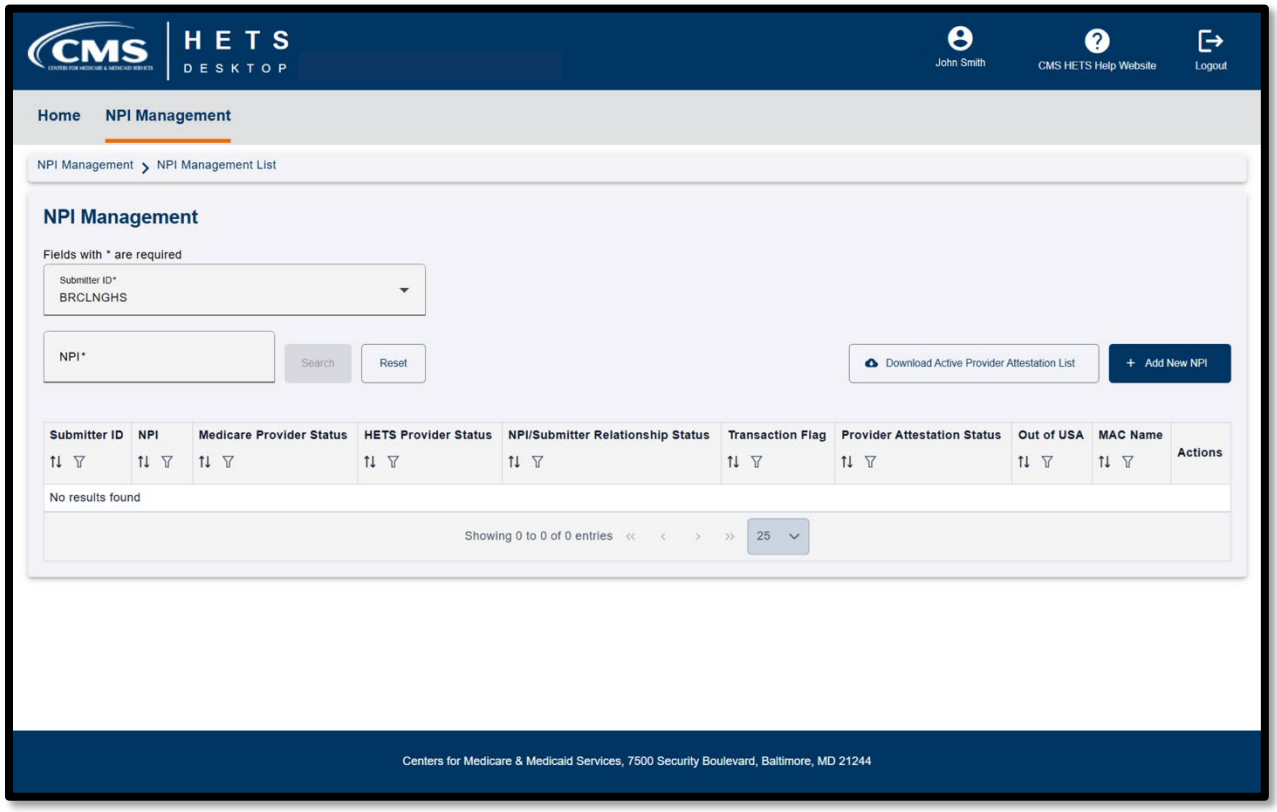

Figure 35: HDT NPI Management Screen – Add

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 36: 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].

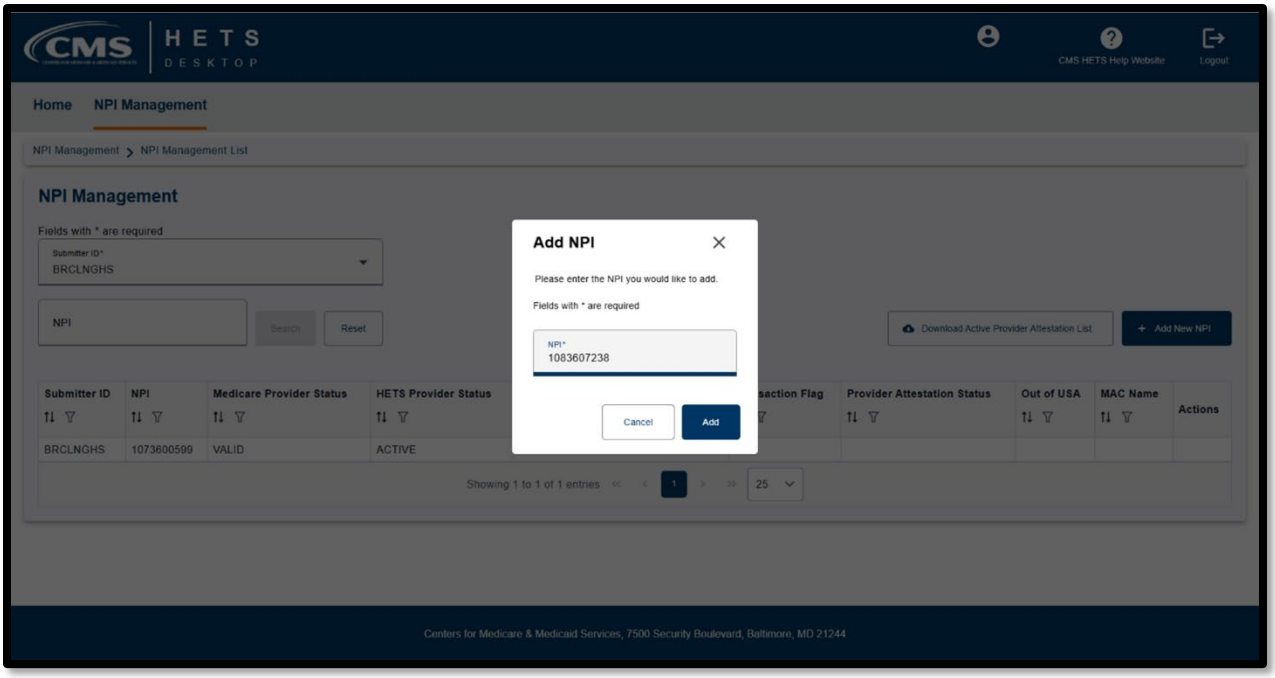

Figure 36: HDT NPI Management Screen – Add NPI

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

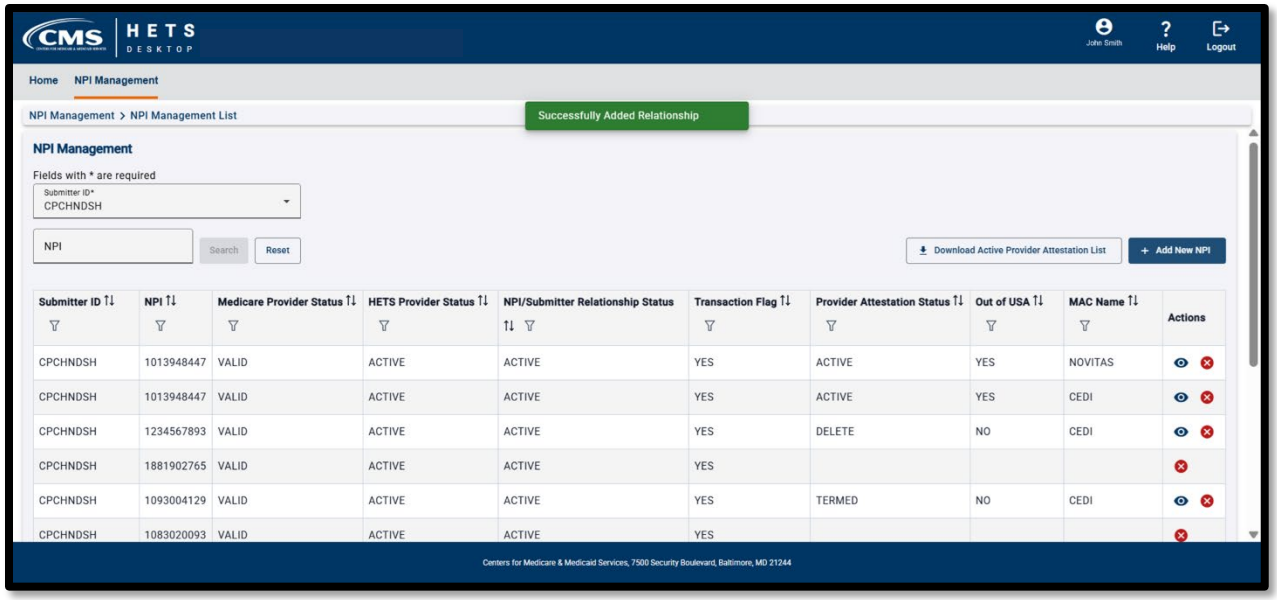

Figure 37: HDT NPI Management Screen – Add NPI Results Sample Responses

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 sending 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 38: HDT NPI Management Screen – Terminate Action*.

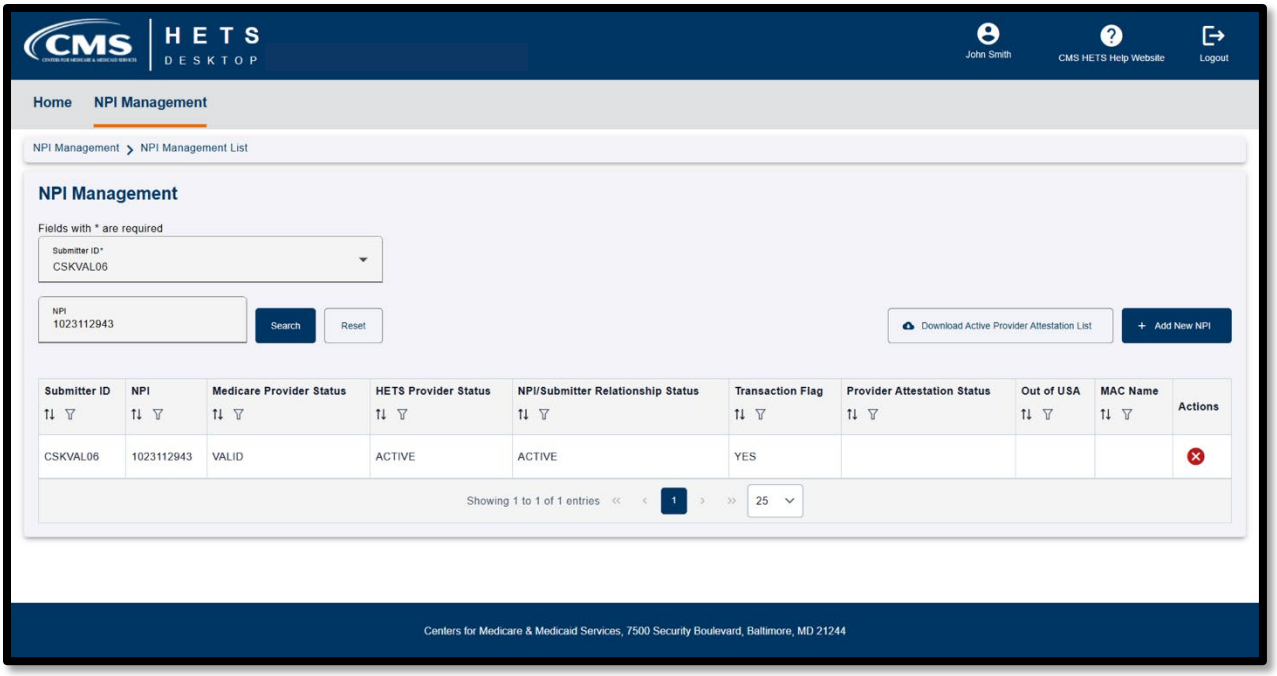

Figure 38: HDT NPI Management Screen – Terminate Action

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 can terminate it 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 39: 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].

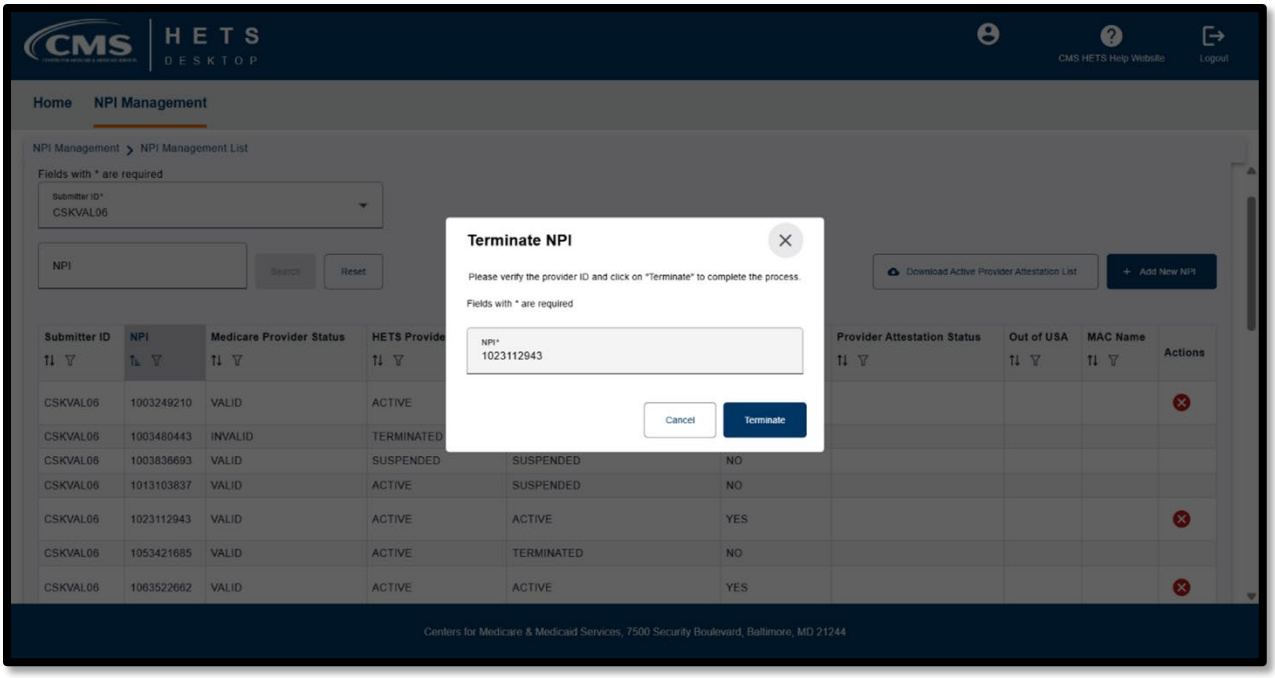

Figure 39: HDT NPI Management Screen – Terminate NPI Action

1.8.1.3.2 Result

HDT will display the NPI relationship termination status as a pop-up on the screen and 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 40: HDT NPI Management Screen – Terminate Results displays the results for the terminate action.

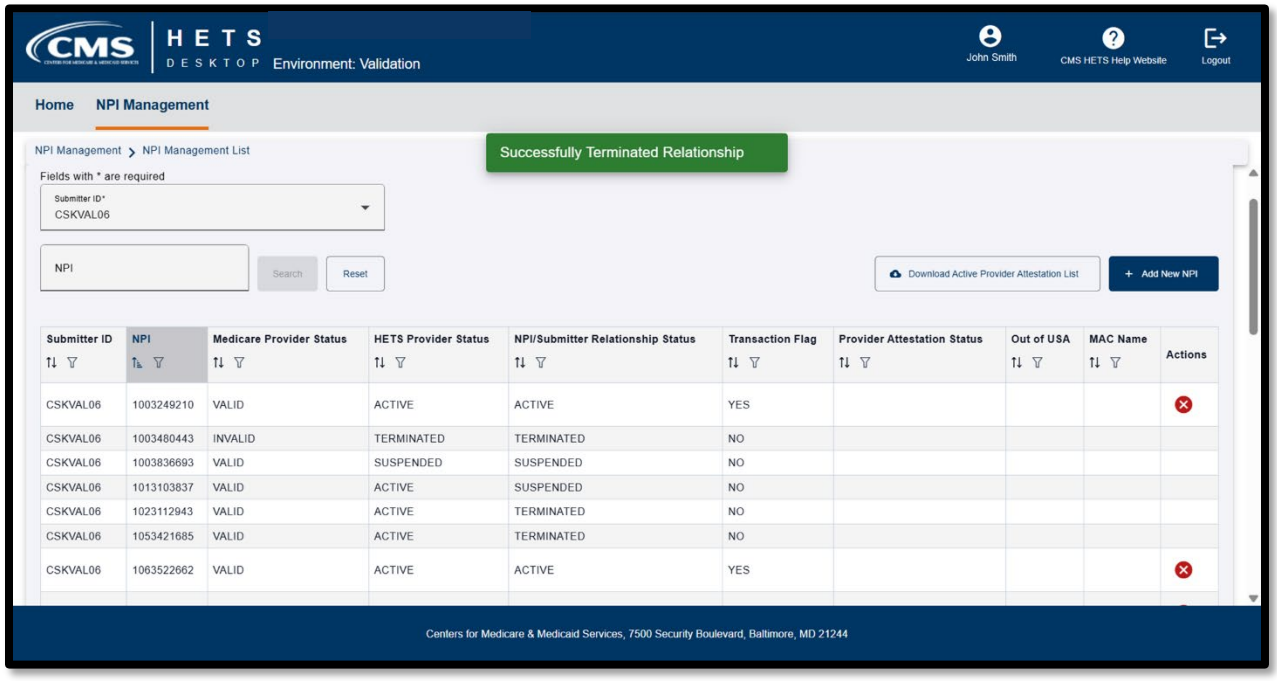

Figure 40: HDT NPI Management Screen – Terminate Results

1.8.1.4 Download Active Provider Attestation List

Vendor or 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. Vendor or 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 41: Download Active Provider Attestation List*.

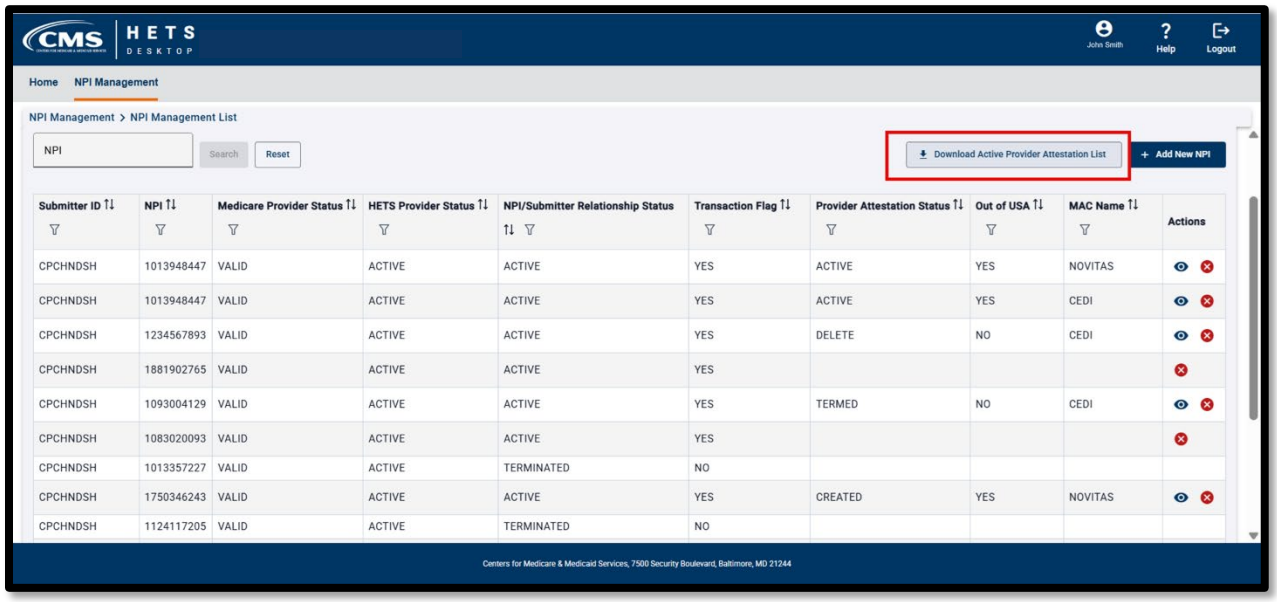

Figure 41: Download Active Provider Attestation List

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 vendor or 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 vendor or Clearinghouse Submitters. This feature enables users to simultaneously query, add, and/or terminate relationships associated with multiple NPI numbers.

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: Vendor or Clearinghouse Submitters may upload only one batch file per day. If a vendor or 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 42: NPI Batch Management Navigation* below.

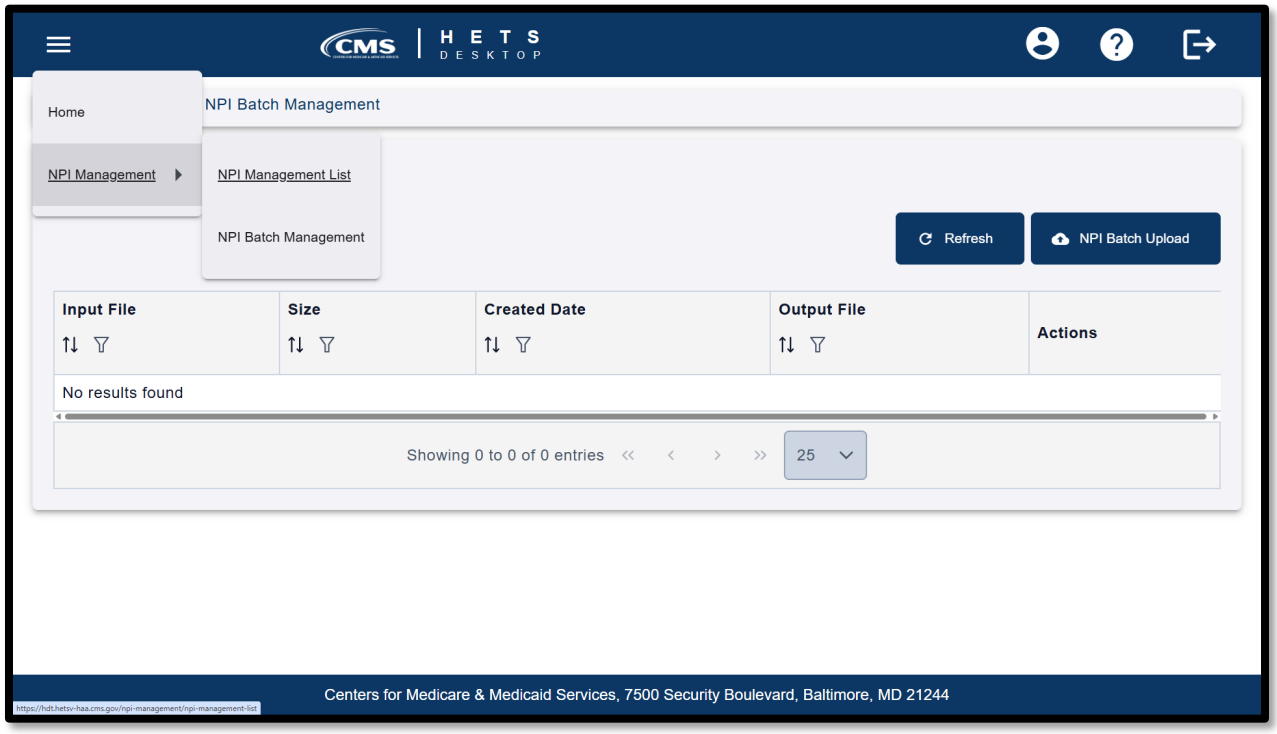

Figure 42: NPI Batch Management Navigation

The HDT NPI Batch Management Screen displays as described in *Figure 43: NPI Batch Management Page*.

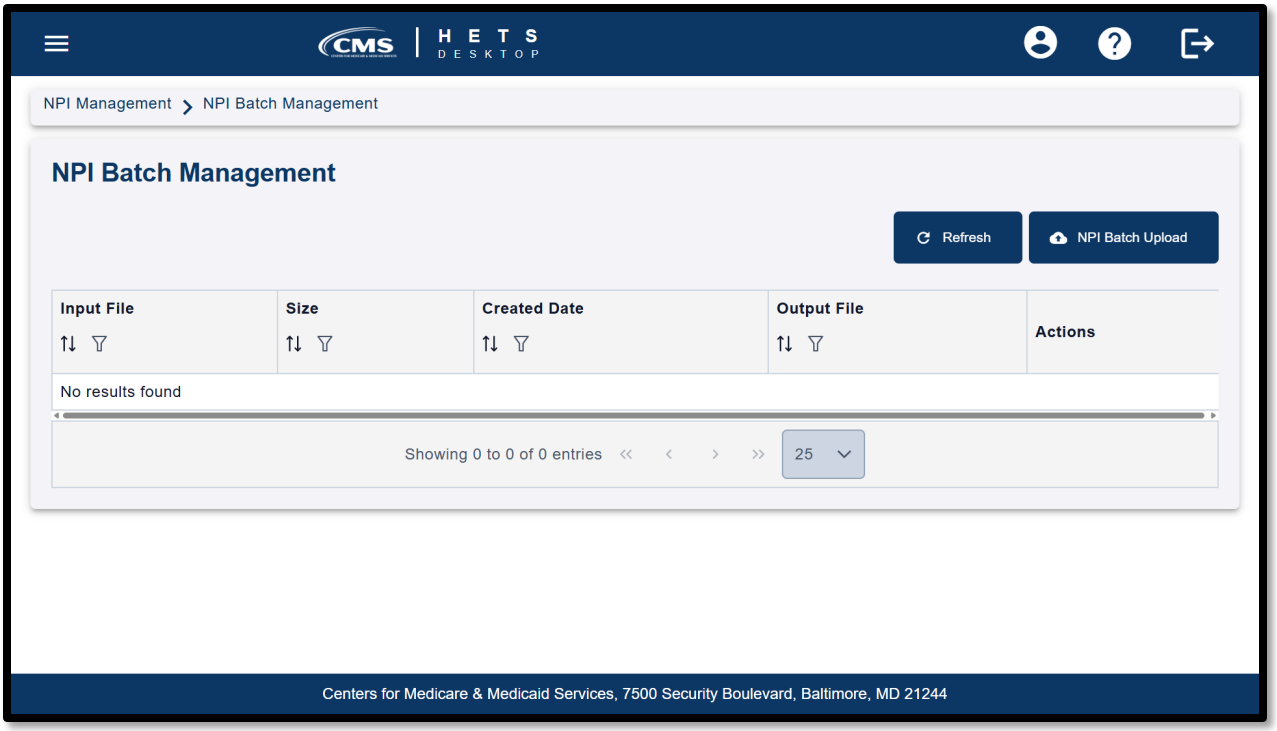

Figure 43: NPI Batch Management Page

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 vendor or Clearinghouse.
NPI	Numeric	10	N/A	The 10-digit NPI to which the vendor or Clearinghouse sends eligibility transactions for the HETS 270/271 application.
Action	Alpha	1	Q, A, or T	The action requested by the vendor or 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 vendor or Clearinghouse.
NPI	Numeric	N/A	The NPI that the vendor or 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 44: HDT NPI Batch Management Screen*.

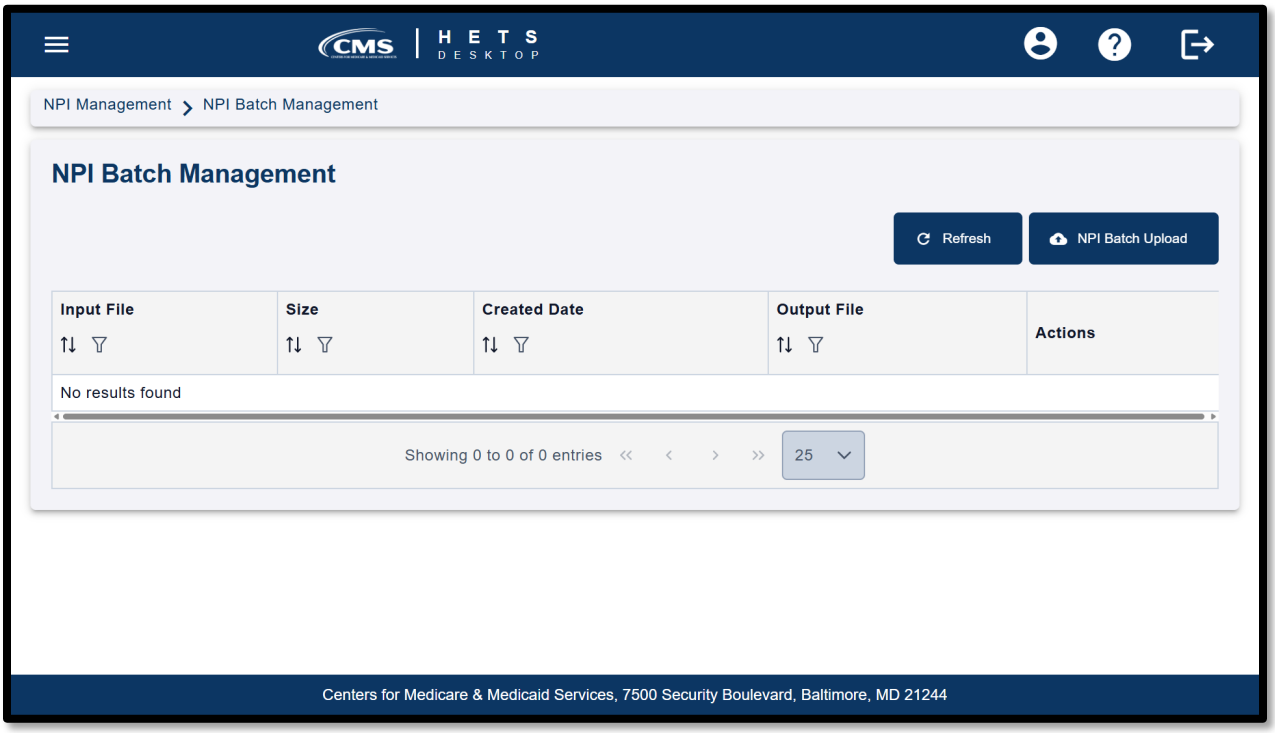

Figure 44: HDT NPI Batch Management Screen

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 45: Select Upload File for Processing* and allow you to select the file from your local device.

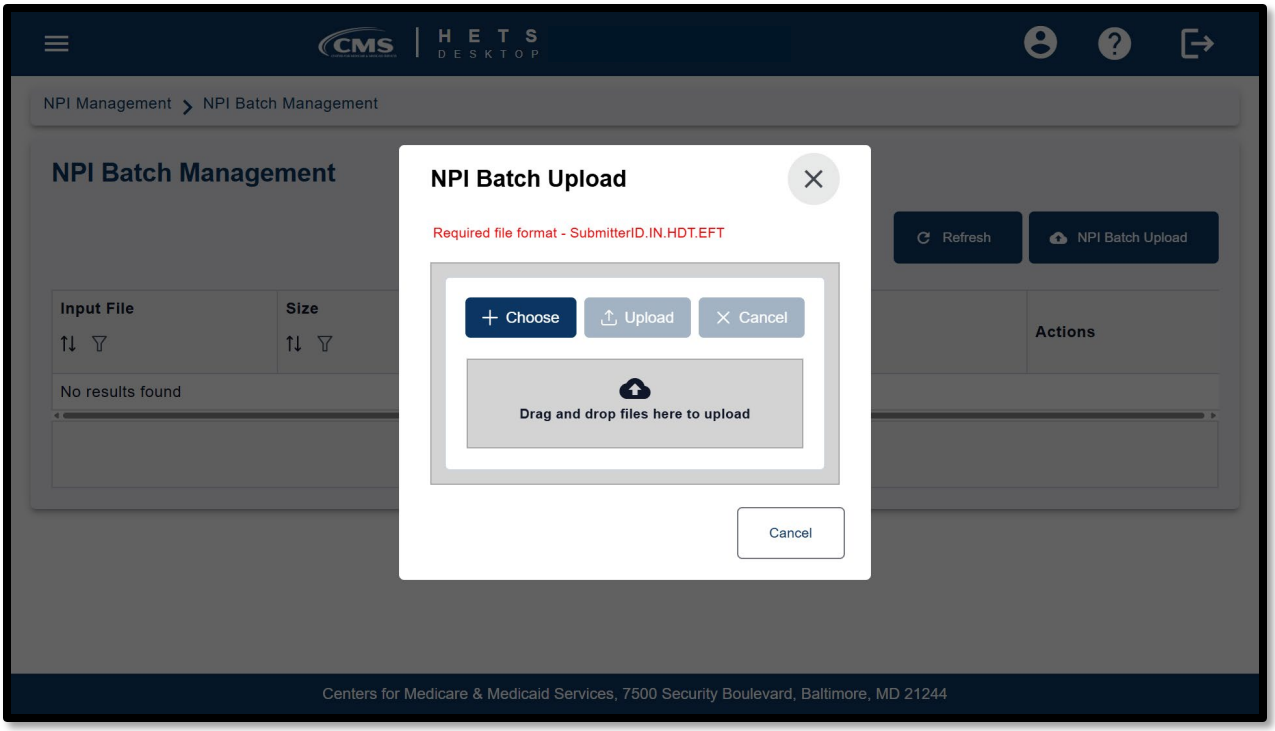

Figure 45: Select Upload File for Processing

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 46: Upload File Selected*.

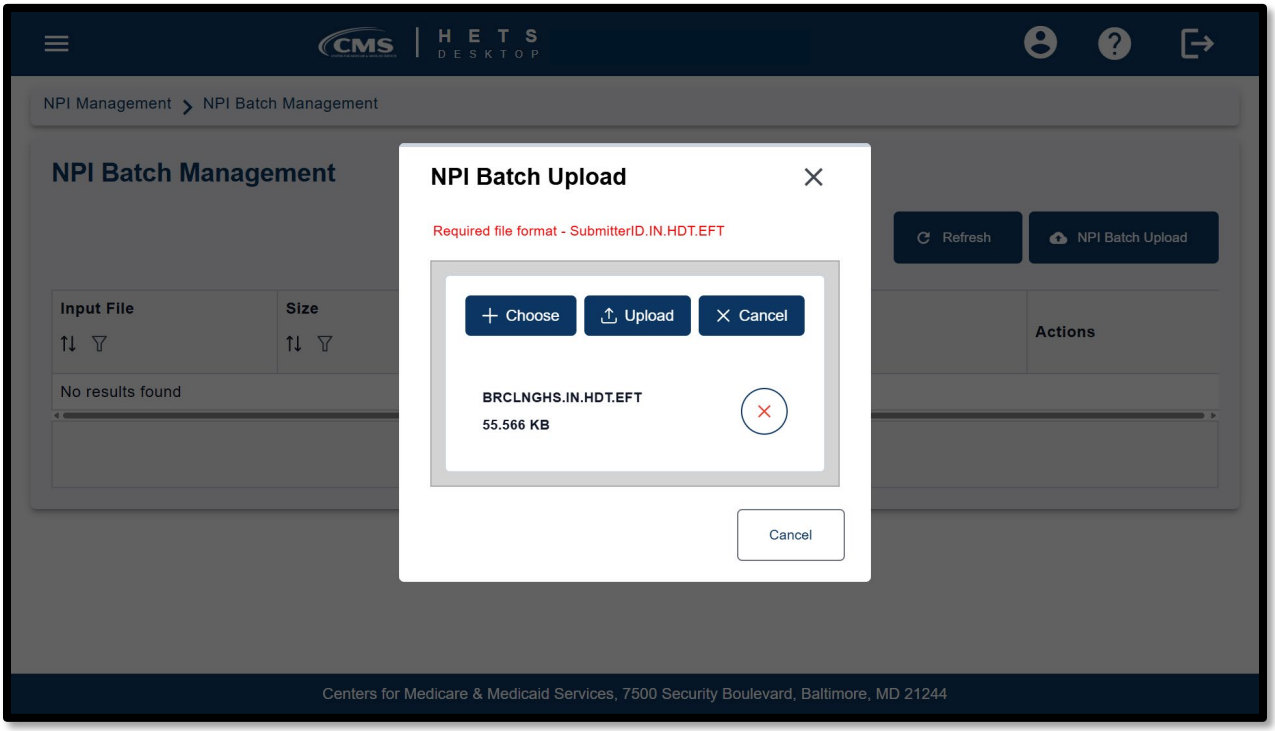

Figure 46: Upload File Selected

3. Select [Upload]. Once the file has finished uploading, HDT will display the message “The batch file uploaded successfully.” See *Figure 47: Batch File Submitted*.

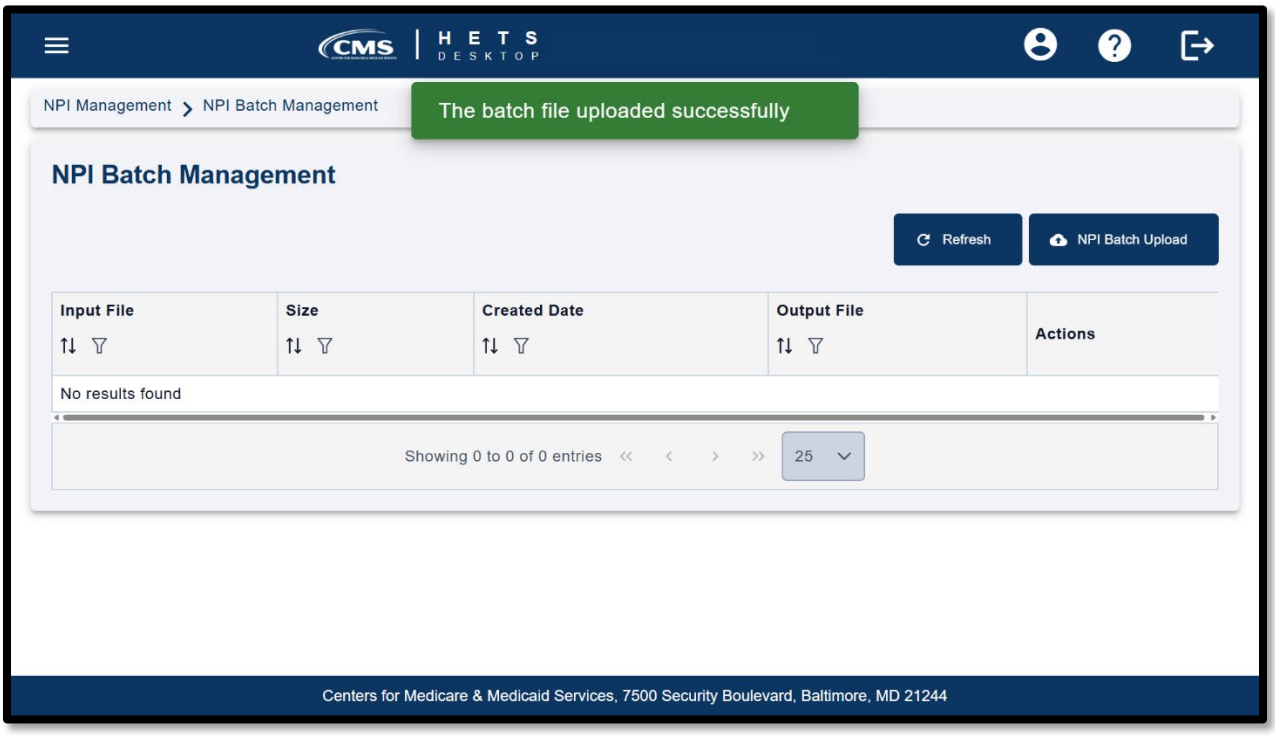

Figure 47: Batch File Submitted

4. The screen will also update to show the file in process, as illustrated in *Figure 47: Batch File Submitted*. Recent batch files will display essential details, including the input file name, file size, creation date, and, if available, the output file name. Completed batch files will have a Download file action available.

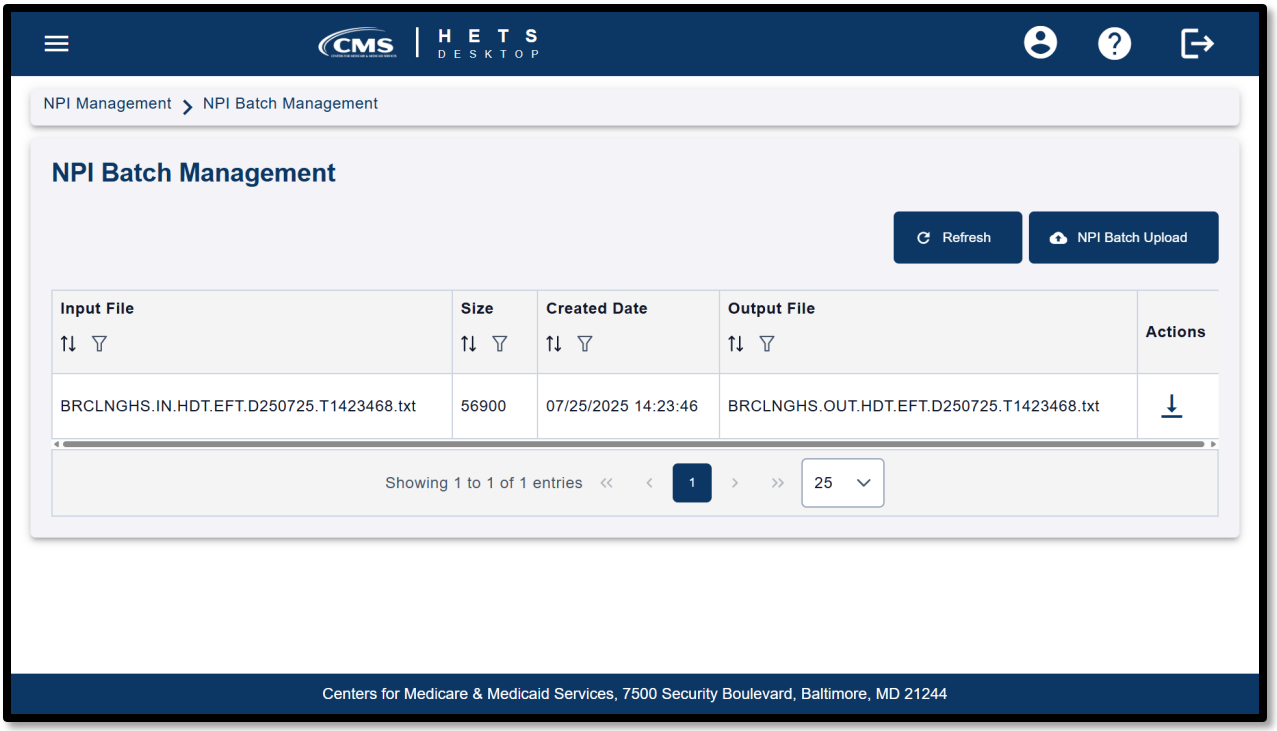

Figure 48: Batch File in Progress

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 49: Batch File Downloaded Successfully*. The file will be downloaded to your machine's default download location. The file will be saved with the default HDT Batch output file name.

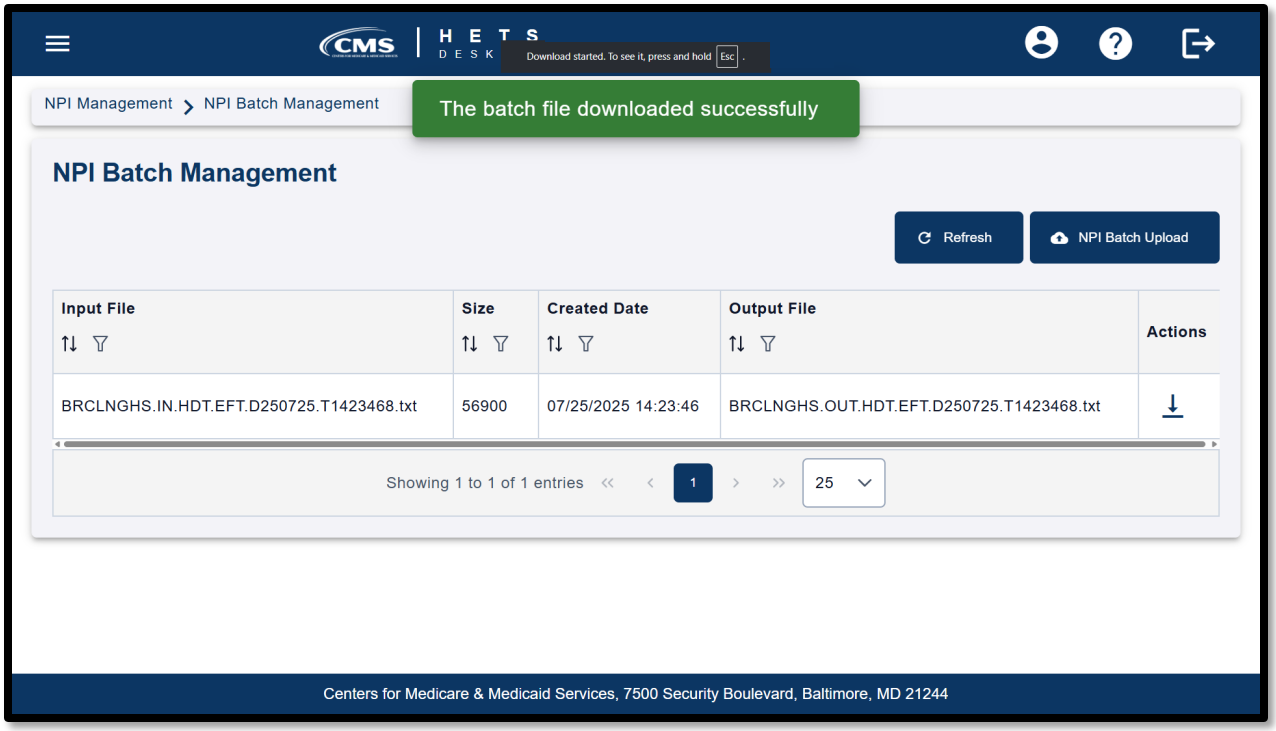

Figure 49: Batch File Downloaded Successfully

1.9.3 Invalid File Name Format Error

If an HDT user from a vendor or 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 50: Invalid File Name Format*.

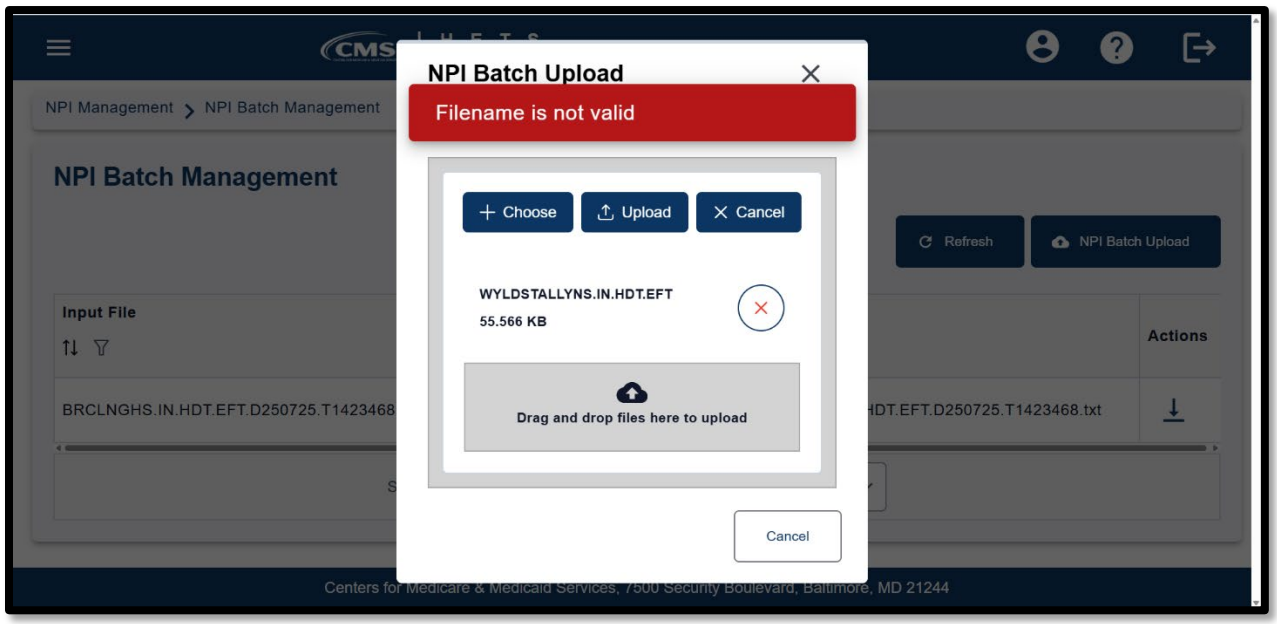

Figure 50: Invalid File Name Format

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 re-upload the file once 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 the *HDT Troubleshooting & Support Information* section.

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

Vendor or Clearinghouse Submitters are limited to uploading one batch file per day. If a vendor or 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
3.0	12/18/2025	TW document review, finalization, and baselining.
2.1	12/16/2025	CMS now permits prospective new HDT users to apply for access using Login.gov credentials. Previously, the use of CMS's IDM was required. New HDT users can now choose to use IDM or Login.gov credentials to apply for HDT access. Note that the MCARE Help Desk, which supports HETS and HDT, cannot assign any Login.gov account issues. Existing HDT Users who may also have a Login.gov account will continue to use their IDM credentials for HDT until they are advised at a future date that they may use Login.gov. No changes to HDT functionality aside from the Login.gov option now appearing on login screens. Document updated to include references to Login.gov, including Login.gov self-support information.
2.0	09/4/2025	The document was updated to remove duplicative information already included in the 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 and 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.

Version Number	Date	Description of Change
1.7	11/16/2023	Updated the following: Removed Contract Number and Document Number. Section 1.3 provides 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.
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.