Centers for Medicare & Medicaid Services

HETS Desktop (HDT) User Guide

Version 4.1

6/8/2026

Table of Contents

List of Figures

List of Tables

1.1 Introduction

This HDT User Guide provides the information necessary for vendors and Clearinghouses 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. 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 must 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:

- Individuals working for or on behalf of HETS vendors or Clearinghouse Submitters ONLY. Individuals working for or on behalf of Medicare Administrative Contractors (MACs) OR Medicare Providers and/or Suppliers that utilize a MAC portal or IVR for eligibility OR direct Medicare Providers and/or Suppliers that directly submit transactions to HETS without interface with a vendor or Clearinghouse aggregator do not utilize HDT.
- 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 vendors or Clearinghouse Submitters to ensure they send only active, valid Original Medicare National Provider Identifier (NPI) numbers to the HETS 270/271 application.

Previously, HETS Submitters utilized HDT to register and maintain records of their business relationships with their HETS 270/271 Provider and/or Supplier customers before submitting HETS 270/271 transactions. Additionally, Submitters could verify whether NPI numbers are eligible for use with the HETS 270/271 application.

Effective in 2026, HDT is used **only** by HETS vendors or Clearinghouse Submitters. HETS eligibility requests from NPIs that do not have a proper Medicare Provider/Supplier HETS EDI Enrollment (or 'attestation') agreement on file with a MAC will result in no better than a HETS 271 AAA error. HETS vendors or Clearinghouse Submitters may use HDT to research HETS EDI Enrollment status and determine whether and why an NPI is eligible for use with HETS. HETS vendor or Clearinghouse Submitters no longer create or manage SID/NPI relationships via HDT. Similarly, HETS vendor or Clearinghouse Submitters also no longer upload or download relationship batch files via HDT.

This user guide addresses actions in 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 *the Referenced Documents* for additional information on IDM and Login.gov.

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 Submitter ID/NPI HETS EDI Enrollment status
- Downloading a list of active NPI/Submitter HETS EDI Enrollments associated with your organization. These enrollments or attestations are created by Medicare Providers or Suppliers
- Troubleshooting common HDT errors

1.1.3 Identity Management (IDM) System Overview

The IDM system enables business partners to request and obtain a single IDM 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 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 but need to re-establish access must 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 joint 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 across the government and the private sector. Today, the Login.gov program is operated as a standalone division within 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:

- View a list of associated NPIs and their HETS trading status.
- Query the status for one or more NPIs via NPI management.
- Download a list of all active Medicare Provider/Providers and Suppliers who created HETS EDI enrollments (attestations) associated with their HETS Submitter ID.

HDT validates NPIs queried by the Submitter to ensure they are valid Original 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 HETS EDI Enrollment (attestation) between the HETS 270/271 Submitter and the Original Medicare Provider or Supplier.

HDT allows manual management of NPIs. NPI management allows vendor or Clearinghouse Submitters to query HETS EDI Enrollment records with Providers and/or Suppliers, one NPI at a time.

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 Original Medicare Provider at the time the request is processed, or c) does not have an associated HETS EDI Enrollment (attestation) 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.

Medicare Providers and Suppliers that intend to submit Original Medicare eligibility requests via a HETS vendor or Clearinghouse must enroll and attest to a known trading agreement with one or more HETS vendors or Clearinghouses. Original Medicare Providers and Suppliers create these attestations using the URLs for their MAC jurisdiction, provided on this page. HETS vendor or Clearinghouse Submitters must inform the customers of the HETS EDI Enrollment requirement to ensure they maintain HETS access. Vendors or Clearinghouses can track the enrollment status of your customers' NPIs using HDT.

- HETS vendor or Clearinghouse Submitters must collaborate with their Medicare Provider/Supplier customers to ensure that HETS EDI Enrollments (attestations) are recorded and maintained via the URLs per MAC jurisdiction provided on this page.
- HETS direct Provider or Supplier Submitters do not create HETS EDI Enrollments (attestations) for their NPIs; these organizations should contact MCARE when an NPI needs to be added or removed from your NPI list.

- Medicare Provider/Supplier NPIs that either a) do not use HETS or b) are only sent to HETS by non-vendor or Clearinghouse Submitters do not need to create HETS EDI Enrollment (attestation) records.

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 download a list of your customers' active HETS EDI Enrollments (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
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

Questions	Answers
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 on a desktop or laptop computer may need to install software updates or configure their web browser 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 users of mobile devices.

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 Submitters will be granted permission to access the HDT application. Users must be associated with a vendor or Clearinghouse Submitter 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 the HDT website.
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]

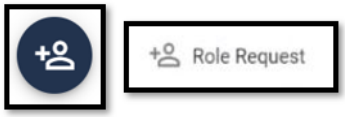

Figure 2: Role Request Button and Role Request Taskbar Option

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.

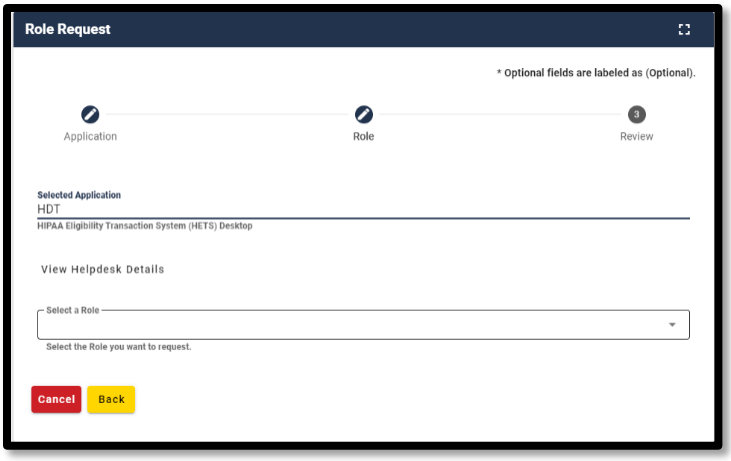

Figure 3: Role Request that Requires Application and Role

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

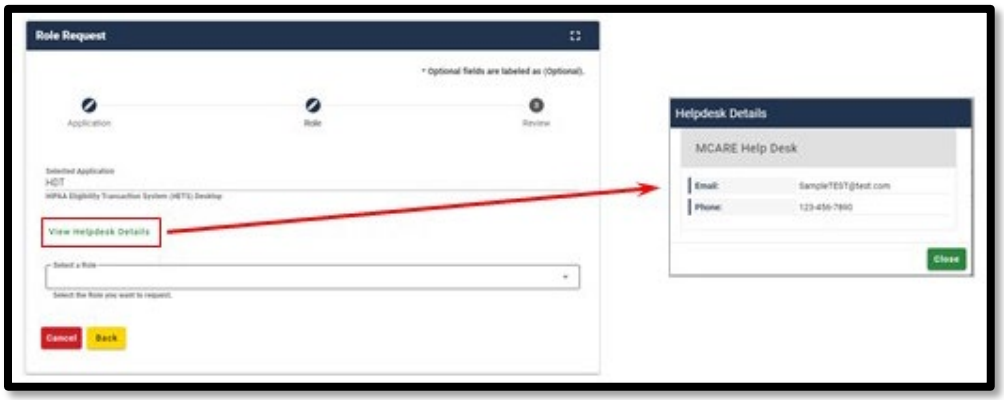

Figure 4: Role Request Helpdesk Details (Optional Step)

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.

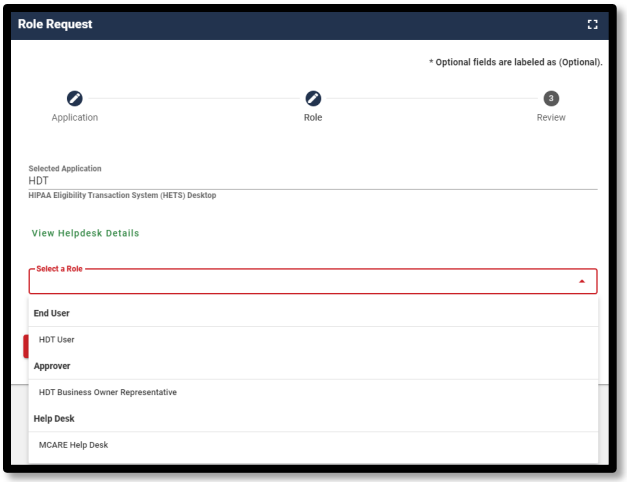

Figure 5: Role Request Specifying HDT Role

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

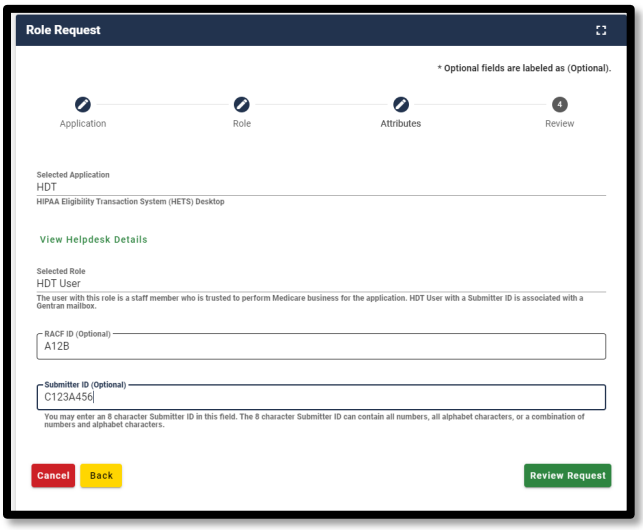

Figure 6: Role Request Specifying Additional Details

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.

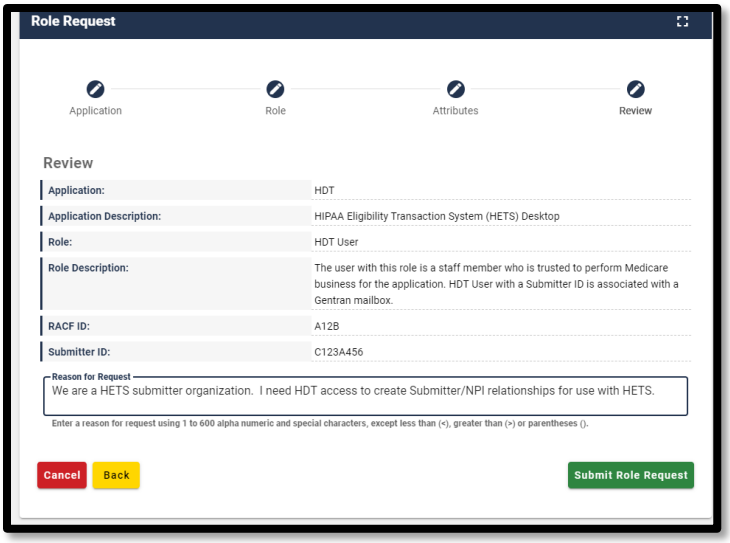

Figure 7: Role Request Ready for Submission

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

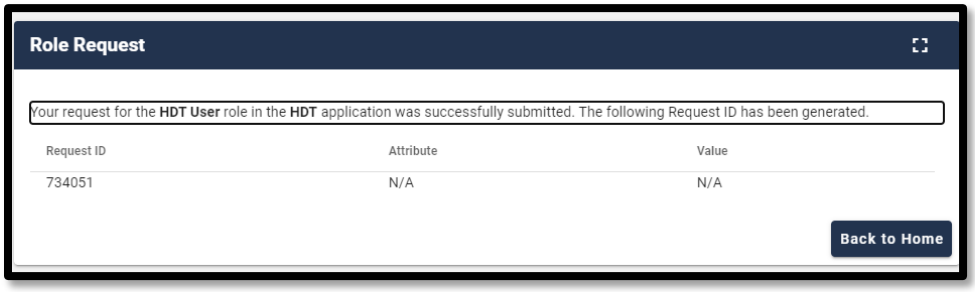

Figure 8: Successful Role Request Message

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.*

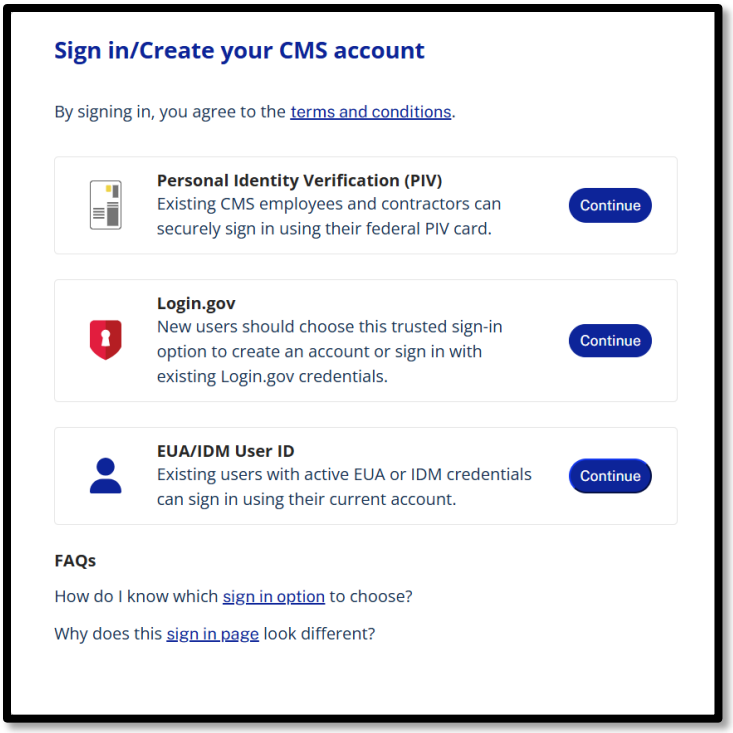

Figure 10: HDT Sign In Window

This document is intended for external users; if you are an external HDT user, please do not select the PIV option.

If you have a Login.gov user account, follow the instructions in Section *1.7.1.2 Login.gov User Log-in Instructions*.

If you have an IDM user account, follow the instructions in *1.7.1.1IDM User Log-in Instructions*.

1.7.1.1 IDM User Log-in Instructions

1. From *Figure 10: HDT Sign In Window* select the EUA/IDM User ID ***Continue*** option. Refer to *Figure 11: IDM User ID Credentials Log In*.

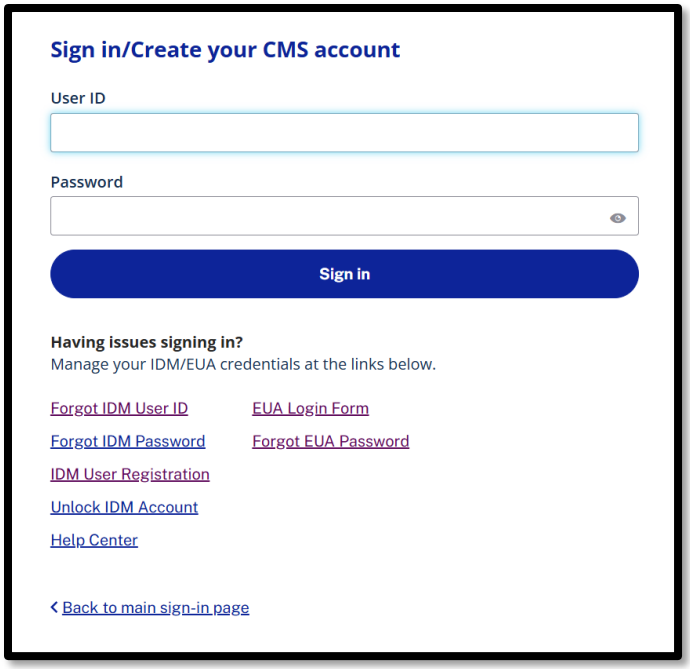

Figure 11: IDM User ID Credentials Log In

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

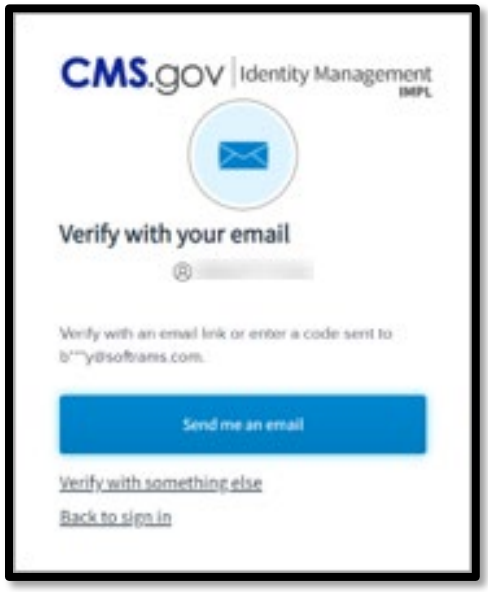

Figure 12: MFA OTP Request Window

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

   The IDM system also supports 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.

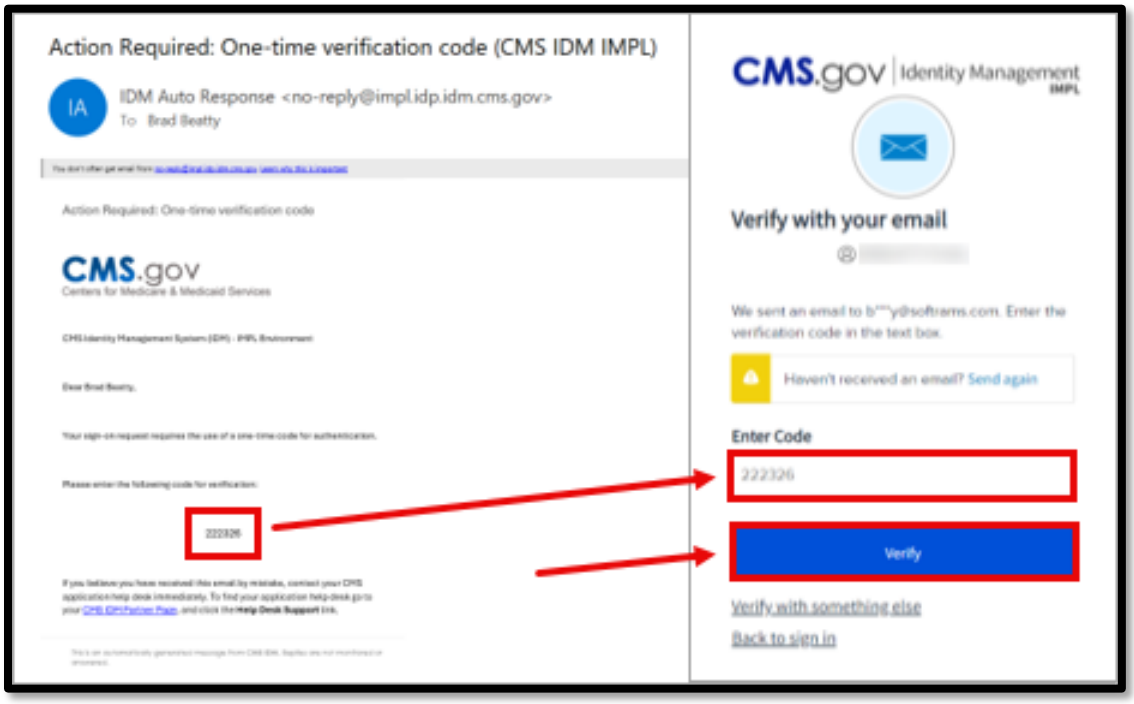

Figure 13: Sample MFA OTP Email and the MFA Verification Window

5. 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 *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.

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 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.

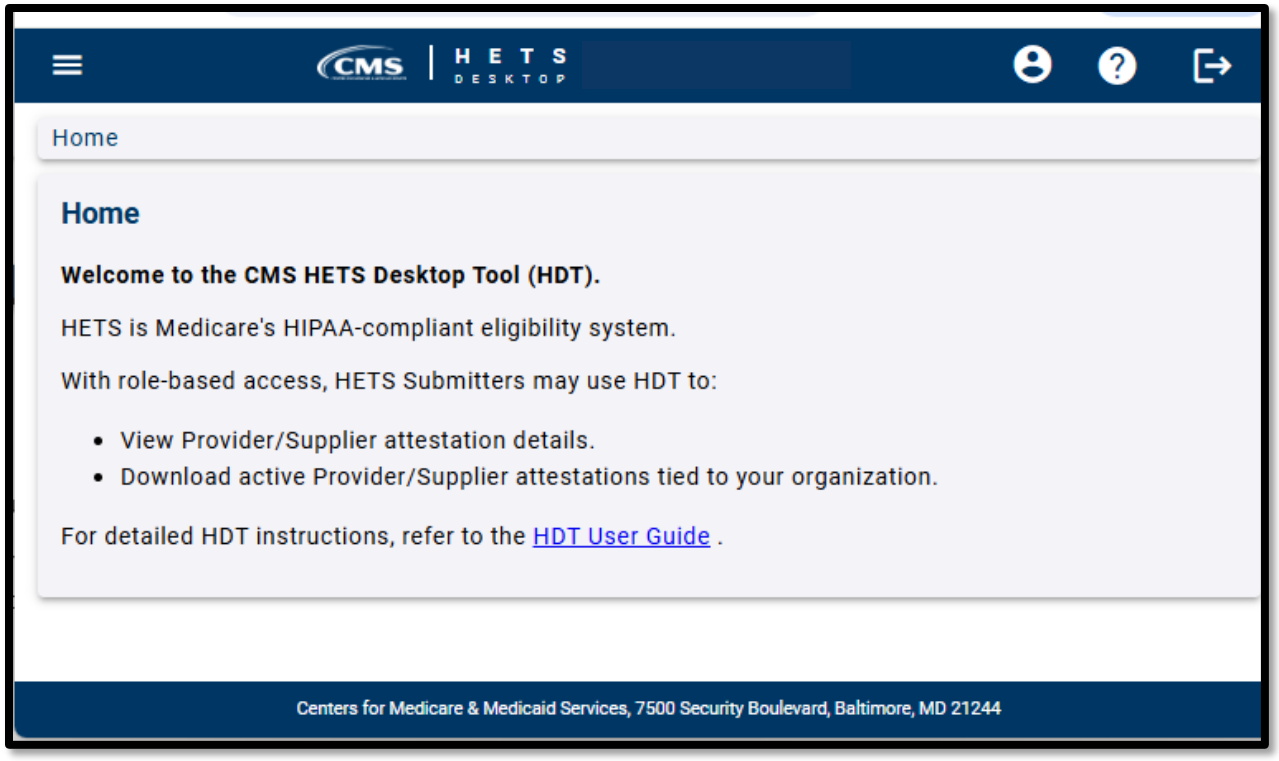

Figure 14: HETS Desktop Home Screen

1.7.1.2 Login.gov User Log-in Instructions

From *Figure 10: HDT Sign In Window* select the Login.gov ***Continue*** option. You will be forwarded to Login.gov, as illustrated in *Figure 15: Login.gov Authentication Window.*

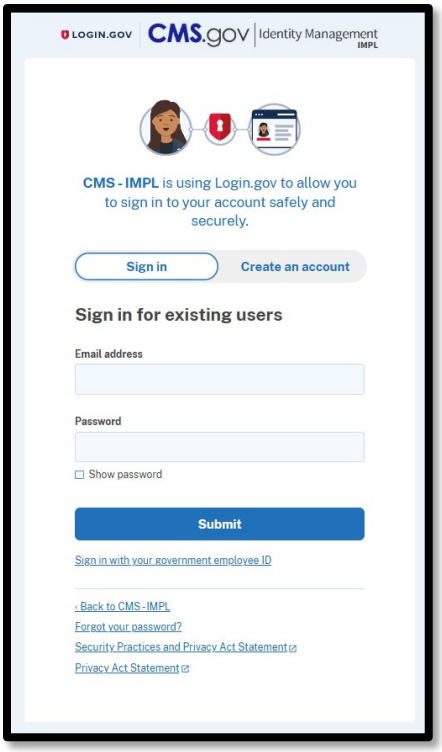

Figure 15: Login.gov Authentication Window

8. Enter your registered Email address and Login.gov Password into the appropriate fields. Check the ***Show password*** box and select the ***Submit*** button.
9. 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)

10. You will then be taken to the HETS Desktop Home Screen as illustrated in *Figure 14: 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 14: HETS Desktop Home Screen.*

Note:

- HDT dynamically optimizes layout and content based on screen display size. Users with limited display space may see some 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 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).

Figure 16: HETS Desktop Home Screen Expanded View illustrates the same HETS Desktop Home Screen page displayed on a larger screen (with the menu removed).

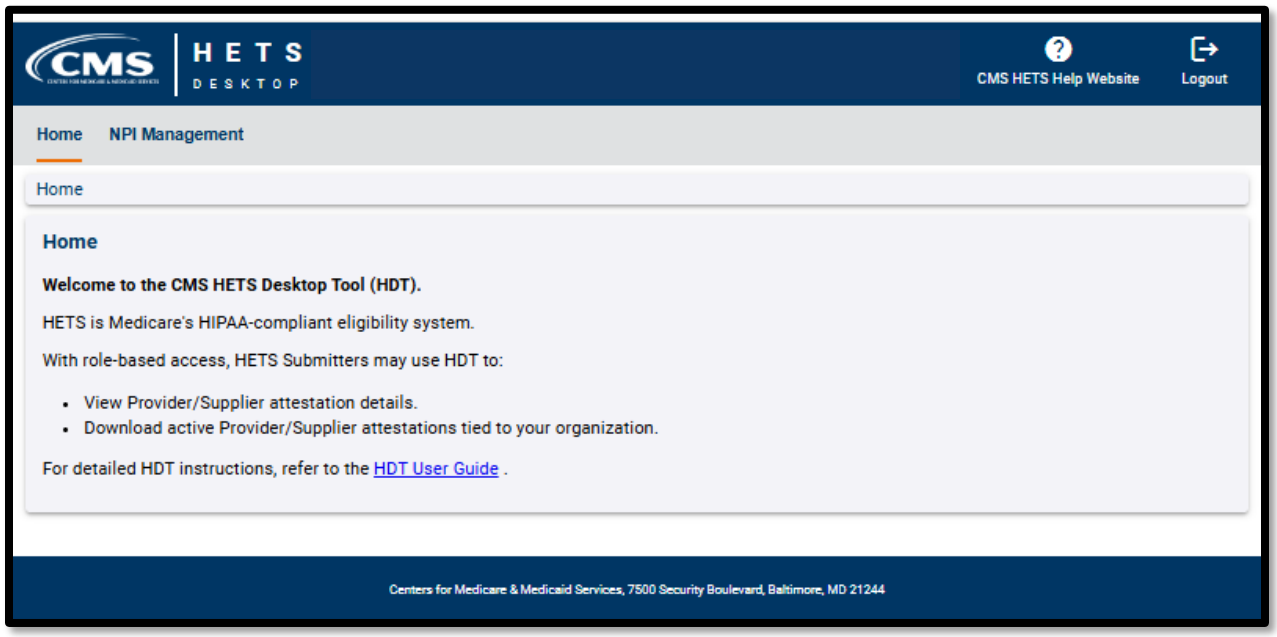

Figure 16: HETS Desktop Home Screen Expanded View

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:** Allows HETS vendor and Clearinghouse Submitters to query NPI numbers one at a time. Query results allow the user to view the HETS EDI Enrollment (attestation) status between a Medicare Provider or Supplier and their organization's HETS Unique ID (if an attestation exists). HETS vendors and Clearinghouse Submitters can also download a list of active attestations associated with their HETS Unique ID.
- **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 23: IDM System Sign In Page*.

1.7.3 Application Layout

HDT dynamically optimizes layout and content based on screen display size. Users with limited display space may see some 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 tabs on the page instead. Similarly, some icons may now contain titles. CMS recommends that HDT users optimize their displays to the maximum readable size.

The navigation options for the HDT application are:

- Home
- NPI Management

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 17: Menu Icon

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

Figure 18: 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 19: CMS HETS Help Website Icon

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

Figure 20: View 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

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 23: IDM System Sign In* **.**

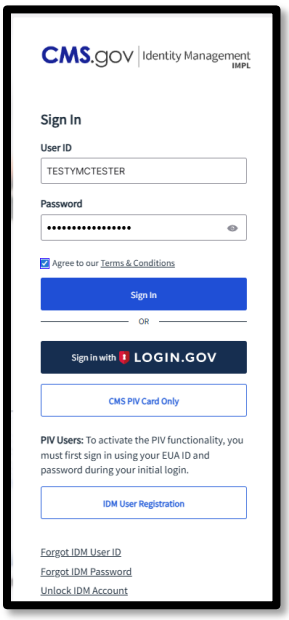

Figure 23: IDM System Sign In Page

1.8 NPI Management

NPI Management allows vendors or Clearinghouse Submitters to query NPI numbers. HETS vendor or Clearinghouse Submitters can view the status of NPIs for use with Medicare and HETS, including if a Medicare Provider has created a related HETS EDI Enrollment. Vendor or Clearinghouse Submitters can also download a list of active HETS EDI Enrollments (attestations) associated with their organization.

To access the NPI Management feature, select ***NPI Management*** from either the menu or the appropriate tab (depending on your screen display size). The display item is displayed in *Figure 24: HDT NPI Management Link.*

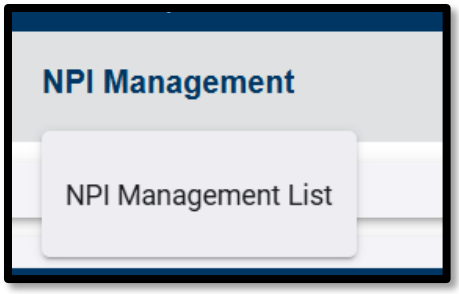

Figure 24: HDT NPI Management Link

1.8.1 NPI Management List

NPI Management allows vendors or Clearinghouse Submitters to query 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 the menu. The **NPI Management List** page is displayed in *Figure 25: NPI Management List Page*.

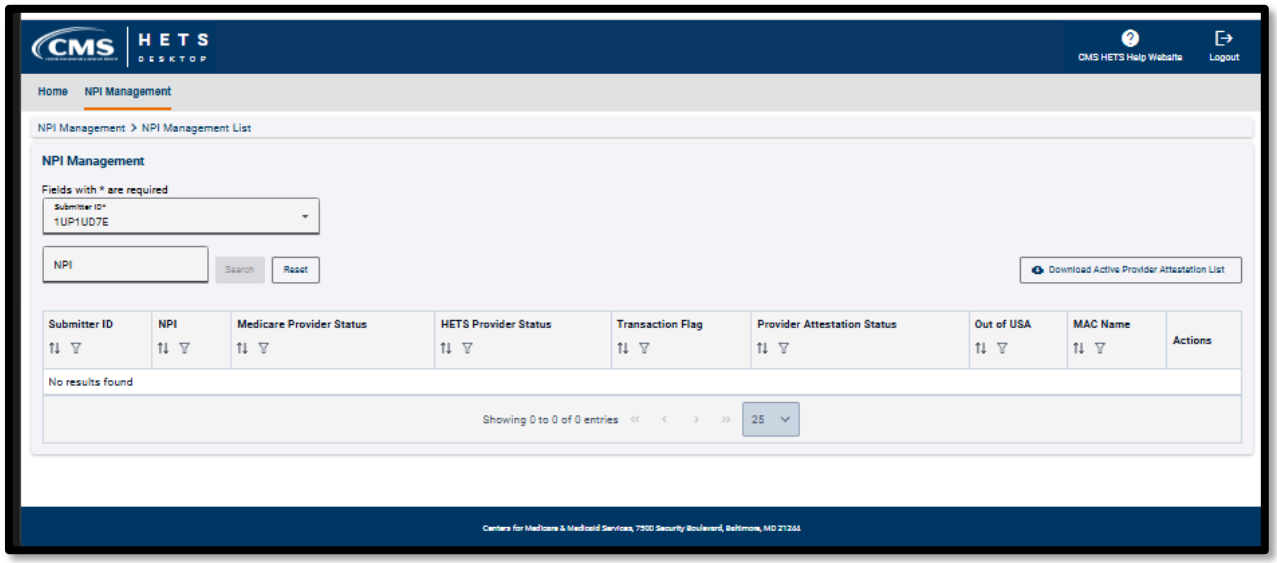

Figure 25: NPI Management List Page

By default, the NPI Management screen displays a table of data associated with the Submitter ID shown. Data in this table are populated from HETS EDI Enrollment (attestations). In the figure above, there are no HETS EDI 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 26: HDT NPI Management Screen – Search Results*.

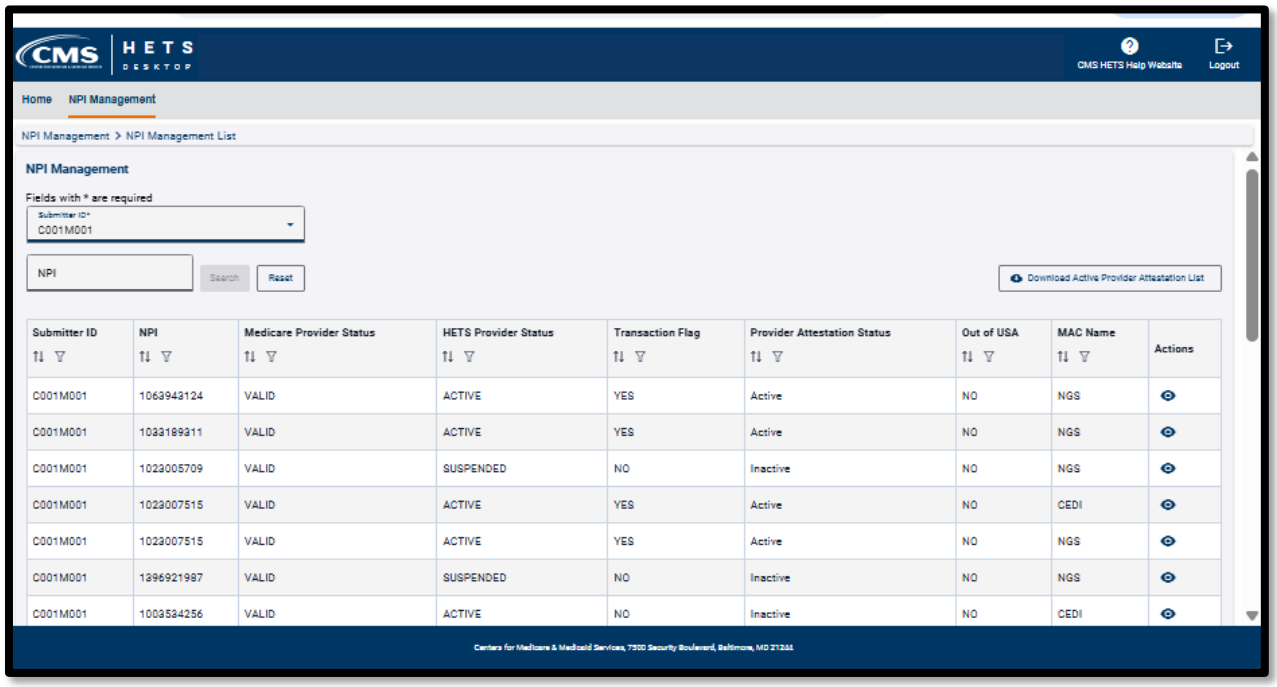

Figure 26: HDT NPI Management Screen – Search Results

4. Results for requested actions are displayed in an NPI Results table, as illustrated in *Figure 27: HDT NPI Management Screen – NPI Entered Search Results*.

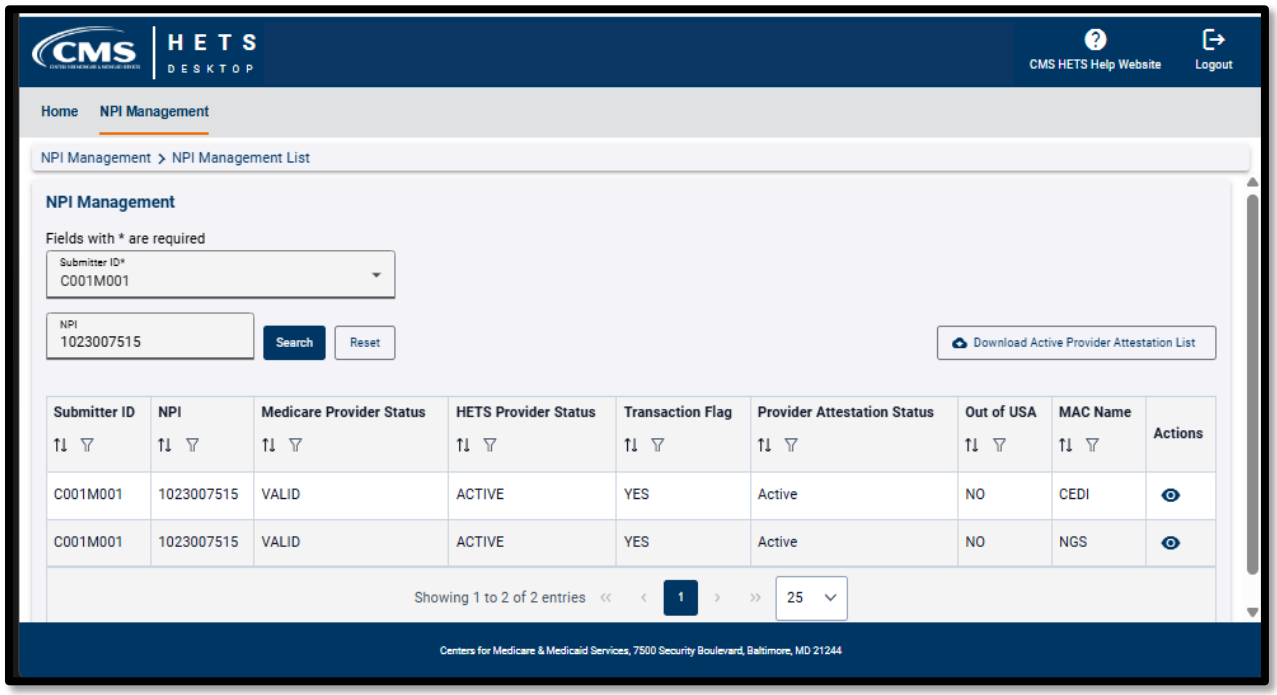

Figure 27: HDT NPI Management Screen – NPI Entered Search Results

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 Original Medicare Provider.	• Values include: • Valid: the Provider is an active, valid Original Medicare Provider or Supplier. • Invalid: the Provider is not an active, valid Original 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.

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 Provider Attestation 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 • Provider Attestation 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 Enrollment (attestation) created by the associated Medicare Provider or Supplier NPI as it relates to the vendor or Clearinghouse's Submitter ID.	• Active: the HETS EDI Enrollment (attestation) is active for the HETS 270/271 application. • Inactive: the HETS EDI attestation is no longer active for the HETS 270/271 application. • Terminated: the HETS EDI 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 Enrollment by the MAC's deadline. • Deleted: the HETS EDI attestation has been deleted by the Medicare Provider or Supplier. • Created: the HETS EDI 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 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 HETS EDI Enrollment (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 HETS EDI Enrollment (attestation) record. Note: NPIs **do not** need a unique attestation record for each MAC. An attested NPI can be submitted by the HETS vendor or Clearinghouse Submitter regardless of the NPI's MAC jurisdiction.	• 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 a HETS EDI Enrollment (attestation) record 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.

5. If a vendor or Clearinghouse Submitter user wants to review the details of an existing HETS EDI Enrollment record (attestation) that appears in their results table. In that case, they can select the 'View' icon when available. See *Figure 28: HDT NPI Management Screen – Attestation View*.

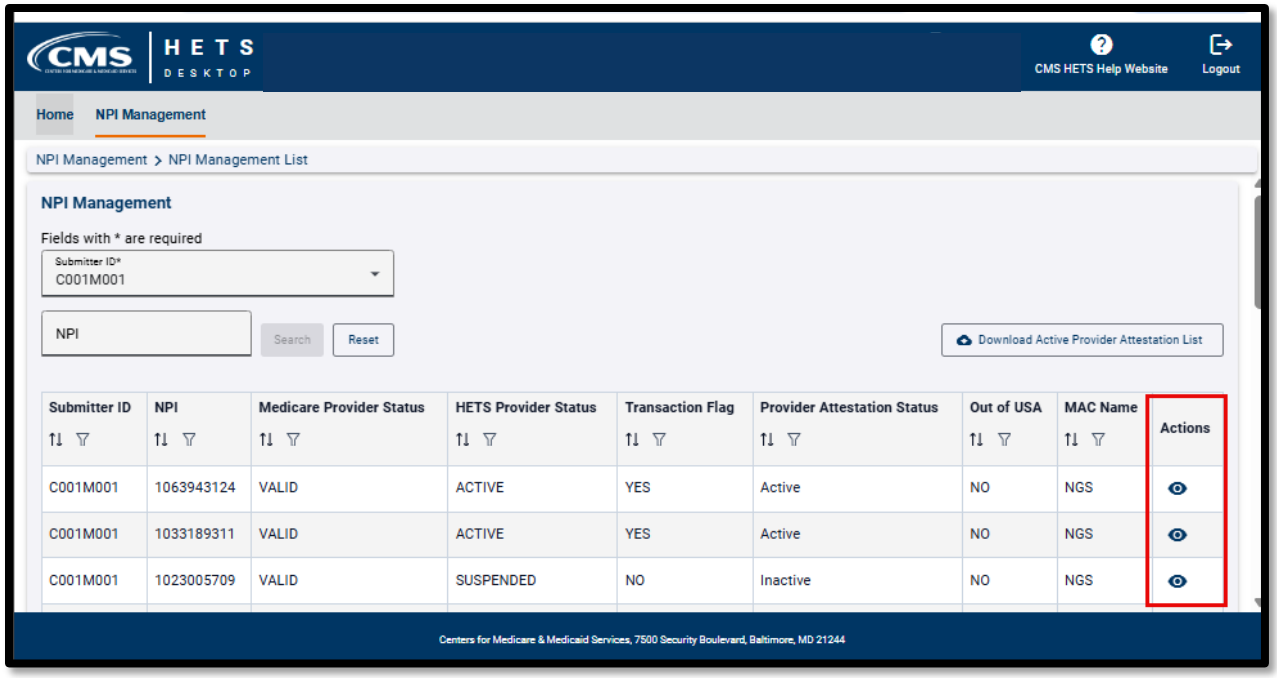

Figure 28: HDT NPI Management Screen – Attestation View

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

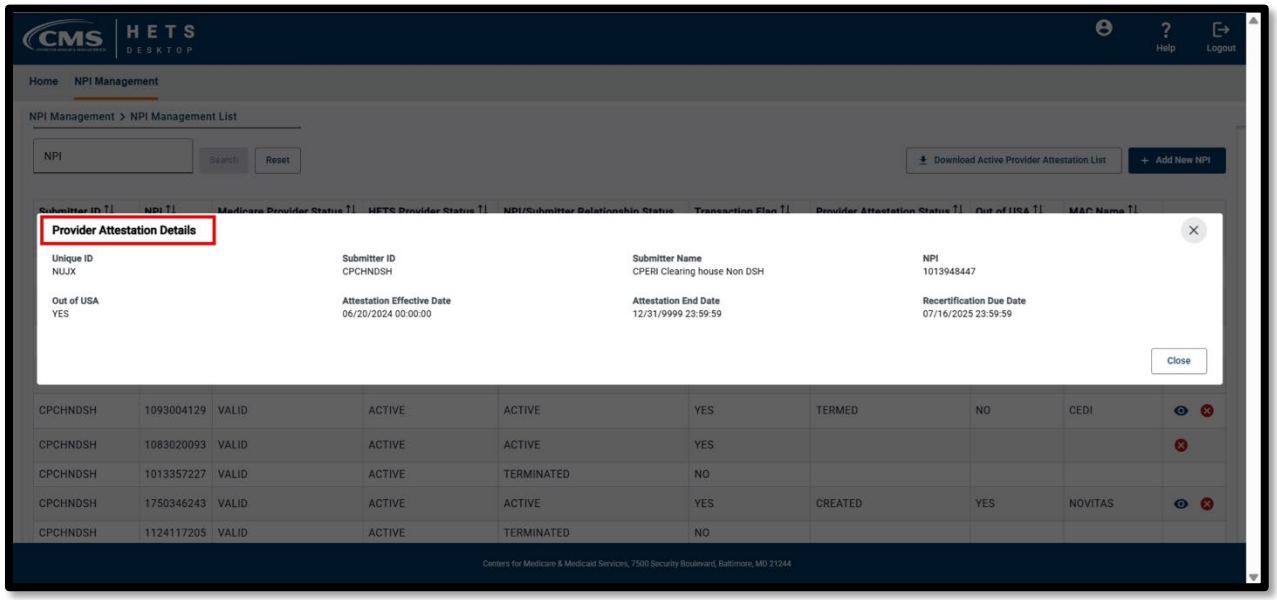

Figure 29: HDT NPI Management Screen – Attestation Detail View

Note: HETS vendor or Clearinghouse Submitters should direct any questions about the content of attestation data to the Medicare Provider or Supplier that created the HETS EDI Enrollment (attestation).

1.8.1.2 Download Active Provider Attestation List

Vendor or Clearinghouse Submitter users can download a list of HETS EDI Enrollments (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 Enrollment records. 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.

1.8.1.2.1 Action

Select [Download Active Provider Attestation List] from the NPI Management screen, as illustrated in *Figure 30: Download Active Provider Attestation List*.

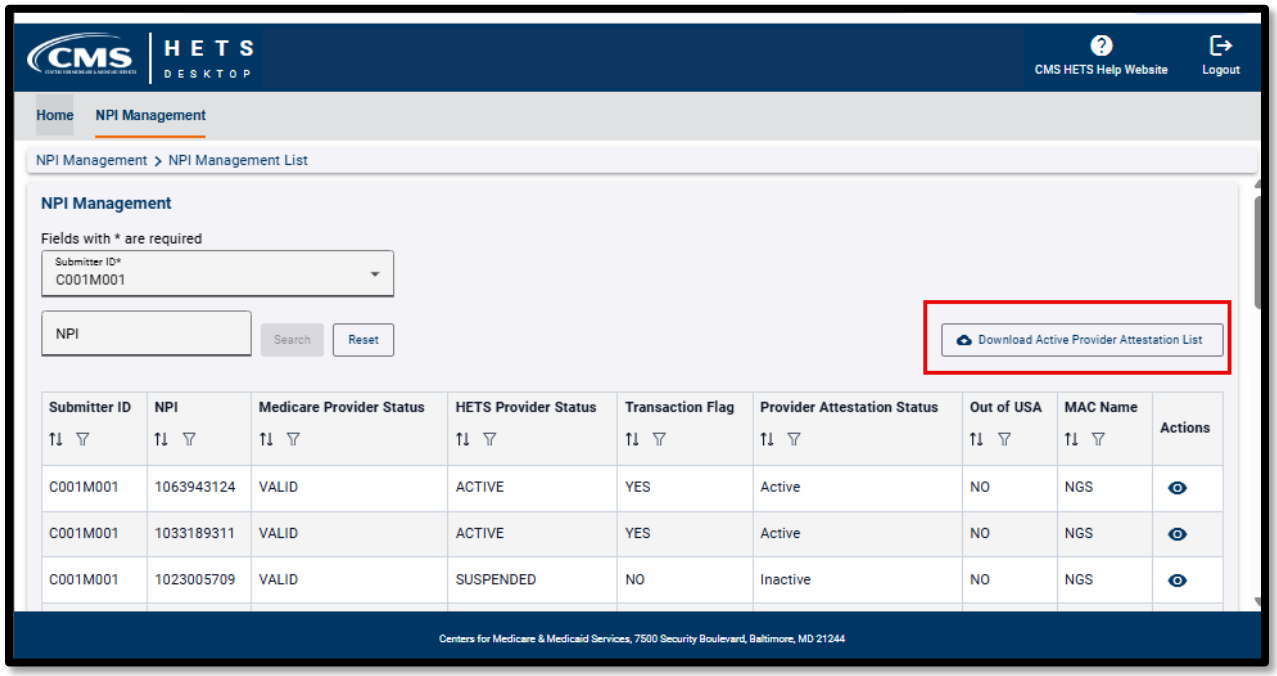

Figure 30: Download Active Provider Attestation List

1.8.1.2.2 Result

A comma-separated file named "Active_Provider_Attestation_Report-aNNNaNNN_YYYYMMDDHHMMSS" (where your organization's HETS Submitter ID is the aNNNaNNN value) 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):

- HETS 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: HETS vendor or Clearinghouse Submitters should direct any questions about the content of attestation data to the Medicare Provider or Supplier that created the HETS EDI Enrollment.

1.9 HDT Troubleshooting & Support Information

1.9.1 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 may be disabled.

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.

1.9.2 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.

1.10 HDT Error Messages

1.10.1 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.

Appendix A: Revision History

Table 3: Record of Changes

Version Number	Date	Description of Change
4.0	4/29/2026	TW document review, finalization, and baselining.
3.1	4/29/2026	Changes include: Removed references to HETS Submitters creating or terminating SID/NPI relationships via HDT. Removed references to NPI Batch Management options. Updated to note that, effective in 2026, HETS utilizes the Medicare Provider or Supplier-created HETS EDI Enrollment (attestation) as part of the real-time HETS Submitter and NPI validation process. HETS no longer uses the HETS SID/NPI combination created by the HETS Submitter using HDT; instead, it relies on the attestation record. HETS continues to verify HETS Submitter status, NPI Original Medicare enrollment status, as well as HETS NPI status for each real-time transaction.
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. The updated document includes references to Login.gov, including self-support information.
2.0	9/4/2025	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.

Version Number	Date	Description of Change
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.