



Centers for Medicare & Medicaid Services 7500 Security Blvd Baltimore, MD 21244-1850

# Health Insurance Portability and Accountability Act (HIPAA) Eligibility Transaction System (HETS) Desktop (HDT) User Guide

Version: 1-11

Effective Date: August 2020

## **REVISION HISTORY**

## **Table 1: Document Revision History**

Version	Date	Description of Changes
1.0	03/19/2016	Baseline Version
1.1	04/29/2016	Updated Version
1.2	06/01/2016	Approved Version
1.3	06/28/2016	Changes include: Section 5.4.2 – Added a clarifying note to indicate that the batch input file must be a comma delimited, flat text file.
		Section 6.3.4 – Removed the last row from Table 6, which previously mentioned a UTF-8 file format requirement. HPG will not return this error and all batch file inputs must be a comma delimited, flat text file.
1.4	08/31/2016	Changes include: Section 4.2 – Added clarifying note that special characters such as @, –, _ and . (dot/period) are not compatible with HDT. Section 4.3.2 – Added clarifying note that special characters such as @, –, _ and . (dot/period) are not compatible with HDT. Section 4.3.4.1 – Removed specific timeframe from Step 8 as the deadline to enter MFA security codes varies by mechanism.
1.5	11/13/2016	Changes include: Section 2 – Updated URLs for EIDM User Guide and EIDM Overview website. Section 4.3 – Updated the official name of the HDT application EIDM user role name from HPG to HDT.
1.6	01/18/2017	Updated Section 2 references for EIDM User Guide and other knowledge resources.
1.7	04/30/2017	Updated Figures 3, 30, 48 and 54 to reflect updated CMS Enterprise Portal Terms and Conditions Screen.

Version	Date	Description of Changes
1.8	11/28/2017	Changes include:
		Changes throughout the document to reflect updates to the CMS Enterprise Portal layout and design.
		Section 2 – Updated URL for EIDM User Guide.
		Section 3.2 – Added note that CMS discourages users from utilizing browser bookmarks with the HDT application.
1.9	07/12/2018	Changes include:
		Section 5.2 – Added Action Result code 'VA' as a potential value returned in HDT. Added NPI/Submitter Relationship Status 'Expired' as a potential value returned in HDT.
		Table 4 – Added Action Result code 'VA' as a potential value returned in an HDT Batch file. Added NPI/Submitter Relationship Status 'E' as a potential value returned in a HDT Batch file.
1.10	03/03/2020	Changes include:
		Section 4.3.6 – Updated the HETS HDT login URL. Effective with the HETS R2020Q100 release, the HDT login URL is now <u>https://cmshdt.cms.gov/HDT/</u> Section 5.3 – This section was rewritten to reflect modified HDT batch processing workflow.
1.11	08/19/2020	Changes include:
		Section 4.1 – Removed references to Internet Explorer.
		Section 4.2 – Updated all references to CMS Enterprise Portal and HDT User ID, password and Username constraints to reflect current CMS and HDT requirements.
		Table 5 – Updated to add '750' error.

## TABLE OF CONTENTS

REVISION HISTORY	
TABLE OF CONTENTS	
LIST OF FIGURES	
LIST OF TABLES	
1. INTRODUCTION	
2. REFERENCED DOCUMENTS	
3. APPLICATION OVERVIEW	
3.1. Conventions	-
3.2. Cautions and Warnings	
4. GETTING STARTED	
4.1. Set-up Considerations	
4.1.2. Google Chrome	
4.2. User Access Considerations	
4.3. Accessing the HDT Application	5
4.3.1. Requesting HDT Access for an Existing CMS Enterprise Portal Accour	
4.3.2. CMS Enterprise Portal New User Registration	
4.3.3. CMS Enterprise Portal User ID and Password Management	
4.3.4. Multi-Factor Authentication (MFA)	
4.3.5. Remote Identity Proofing (RIDP)	
4.3.6. Login to the HDT Application	
4.4. Application Organization & Navigation	
4.5. Exiting the Application	
5. USING THE APPLICATION	
5.1. Application Layout	
5.2. NPI Management (HDT-1001)	
5.2.1. Query	
5.2.2. Add	
5.2.3. Terminate	
5.3. NPI Batch Management	
5.3.1. Input File	
5.3.2. Output File	
5.3.3. Viewing NPI Batch Management	
5.3.4. Uploading a File	62
5.3.5. Downloading Output File	
5.3.6. Invalid File Name Format Error Message	
6. TROUBLESHOOTING & SUPPORT	
6.1. Troubleshooting	
6.2. Connectivity	
6.3. Error Messages	
6.3.1. Access and Behavior Error Messages	
6.3.2. CMS Enterprise Portal Login	
6.3.3. Missing or Invalid NPI	
6.3.4. Batch File Error Messages	
6.4. Special Considerations	
6.4.1. Data Size Limits	68

	6.4.2. Daily Batch File Submission	68
6	.5. System Support Information	
	GLOSSARY	
8.	ACRONYMS	71

## LIST OF FIGURES

Figure 1: CMS Enterprise Portal Login Screen	5
Figure 2: CMS Enterprise Portal Login Screen with Multi-Factor Authentication	6
Figure 3: My Access Screen	
Figure 4: My Access Screen	
Figure 5: Request Access	
Figure 6: Select a Role	
Figure 7: HDT User Role Identity Verification	
Figure 8: Identity Verification Screen	
Figure 9: Terms and Conditions Screen	10
Figure 10: Your Information Screen	11
Figure 11: Verify Identity	12
Figure 12: Complete Set Up	13
Figure 13: Multi-Factor Information Screen	13
Figure 14: Register Your Phone, Computer or Email Screen	14
Figure 15: Complete Set Up	14
Figure 16: Request New Application Access Screen	15
Figure 17: Provide RACF ID, Submitter ID, and Reason for Request	15
Figure 18: Request New Application Access Review	16
Figure 19: Request New Application Access Acknowledgement	16
Figure 20: CMS Enterprise Portal Screen	17
Figure 21: New User Registration	18
Figure 22: Choose your Application	18
Figure 23: Terms and Conditions	19
Figure 24: Register Your Information	20
Figure 25: Choose User ID and Password	21
Figure 26: Registration Summary	22
Figure 27: Confirmation	
Figure 28: CMS Enterprise Portal Screen	24
Figure 29: Login to CMS Enterprise Portal	25
Figure 30: Select My Profile	
Figure 31: Register MFA	26
Figure 32: Select Credential Type	27
Figure 33: Symantec Credential ID	28
Figure 34: Select Phone/Tablet/PC/Laptop as MFA Device Type	29
Figure 35: Select Email as Credential Option	
Figure 36: Select Text as Credential Option	31
Figure 37: Select IVR as Credential Option	
Figure 38: Register MFA Device- Successful Confirmation Screen	33
Figure 39: Unable to Access Security Code Begin Navigation	
Figure 40: Unable to Access Security Code User ID Entry	34

Figure 41: Unable to Access Security Code Challenge Questions	. 34
Figure 42: Unable to Access Security Code Challenge Completion	. 35
Figure 43: Selecting One Time Security Code Option as MFA Device	. 36
Figure 44: CMS Enterprise Portal Screen	
Figure 45: Select My Profile	. 38
Figure 46: Remove Your Phone or Computer	. 39
Figure 47: Removal of Registered MFA Device Complete	. 40
Figure 48: CMS Enterprise Portal Screen	.41
Figure 49: CMS Enterprise Portal Login Screen with Multi-Factor Authentication –	
Access to HDT	
Figure 50: HETS Desktop Home Screen (HDT-1000)	. 43
Figure 51: CMS Enterprise Portal Web Access Management (Logout) Screen	.44
Figure 52: HDT Application Site Map	
Figure 53: HETS Desktop Home Screen (HDT-1000)	. 45
Figure 54: HDT NPI Management Screen (HDT-1001)	. 47
Figure 55: HDT NPI Management Screen (HDT-1001) – Results	. 48
Figure 56: HDT NPI Management Screen (HDT-1001) – Query	. 50
Figure 57: HDT NPI Management Screen (HDT-1001) – Query Results	. 51
Figure 58: HDT NPI Management Screen (HDT-1001) – Add	. 52
Figure 59: HDT NPI Management Screen (HDT-1001) – Add Results	. 53
Figure 60: HDT User Interface NPI Management Screen (HDT-1001) – Terminate	. 54
Figure 61: HDT NPI Management Screen (HDT-1001) – Terminate Results	. 55
Figure 62. NPI Batch Management Menu Navigation	. 56
Figure 63: HDT-1002 NPI Batch Management Screen	. 62
Figure 64: Select Upload File for Processing	
Figure 65: Submitted File – In Progress Verification and Output File	. 63
Figure 66: EFT File Download	. 64
Figure 67: Invalid File Name Format	
Figure 68: Incorrect ID, Password or Security Code Screen	. 67
Figure 69: NPI Management – Invalid NPI Screen	. 67

## LIST OF TABLES

Table 1: Document Revision History	ii
Table 2: Typographical Conventions	
Table 3: Input File Layout and Element Description	
Table 4: Output File Layout	58
Table 5: Access and Behavior Error Messages	66
Table 6: Batch File Error Messages	68
Table 7: Acronyms and Definitions	71

## **1. INTRODUCTION**

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

The 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 are only sending active, valid Fee For Service (FFS) Medicare National Provider Identifier (NPI) numbers to the HETS 270/271 application.

Submitters must utilize the HDT application to register and maintain an up-to-date record of their business relationships with their HETS 270/271 provider and/or supplier customers prior to submitting HETS 270/271 transactions. In addition, Submitters are able to verify if NPI numbers are eligible for use with the HETS 270/271 application.

## 2. REFERENCED DOCUMENTS

The *HETS 270/271 Companion Guide* provides information related to the HETS 270/271 application described in <u>Section 3</u>. Users can obtain the latest version of the HETS 270/271 Companion Guide in the Downloads section at the following website link:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/index

The CMS *Enterprise Identity Management (EIDM) User Guide* provides guidance on how to register, obtain, view and change access to the EIDM system, including the registration approval process. The EIDM system is, for the purposes of the HETS HDT User Guide, referred to as the CMS Enterprise Portal. The EIDM User Guide may be accessed via this website link:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/EnterpriseIdentityManagement/Guides-and-Documentation

If problems and/or questions arise while accessing the HDT application, contact the MCARE Help Desk at 1-866-324-7315 or at <u>MCARE@cms.hhs.gov</u> Monday through Friday, from 7:00 AM to 7:00 PM ET.

## 3. APPLICATION OVERVIEW

Users access the HDT application after authenticating their identity using a CMS Enterprise Portal User ID and password. Approved CMS Enterprise Portal Users must add the HDT role to their CMS Enterprise Portal profile from the CMS Portal Access Catalog then obtain CMS approval before HDT access will be granted.

The HDT application is used by Submitters to:

- Register their HETS 270/271 provider/supplier customers with CMS to establish an NPI/Submitter relationship
- Maintain a list of all NPIs that their organization will be sending to the HETS 270/271 application
- Query the status for one or more NPIs via the HDT application
- Review their current Submitter profile

The HDT application will validate 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 on a daily basis. If an NPI is deemed to be invalid by Medicare, the NPI will also be invalid in HDT and will be prohibited from receiving PHI from the HETS 270/271 application.

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

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

The HDT application allows for both manual and batch NPI management processes.

The manual NPI management options allow Clearinghouse and Direct Provider Submitters to query, add, and terminate their relationships with providers and/or suppliers one NPI at a time. The screen will display the session's most current 25 responses in order, with the most recent response listed first.

The batch NPI management option allow Clearinghouse Submitters to query, add, and terminate their relationships for multiple NPIs at one time. The NPIs must be submitted in a flat text file that can be uploaded to the HDT application through the Enterprise File Transfer (EFT) system. Users are assigned a mailbox in the EFT system and response files are returned to the user's mailbox after the input file(s) has been processed by HDT. The response files are kept in the user's EFT mailbox for a minimum of 30 days before they are archived.

## 3.1. Conventions

This guide provides screen prints and corresponding narrative to describe how to use the HDT application.

Typographical conventions used throughout this guide are described in Table 2.

Convention	Description	Example
Button Name	Square brackets ([]) are placed around the references to the names of all buttons and links displayed on the screen. The button names use mixed-case alphanumeric characters.	[Query]
Screen Name	All screen names will be represented as mixed- case, bold italic text and contain the full description of the screen.	Screen Name
Input	Spaces or locations that accept input on the screens. The input is in the form of mixed-case alphanumeric characters in bold text.	Input
Hyperlink	Fields that (when clicked on) link to another document or website. These fields are displayed in blue and underlined.	<u>Hyperlink</u>
Note	Denotes important information and are represented as mixed-case, underlined text followed by a colon.	<u>Note:</u>

 Table 2: Typographical Conventions

## 3.2. Cautions and Warnings

Web browser capabilities such as back, forward, refresh and logging out should not be used during HDT application sessions. Users should follow the instructions provided in this document. CMS discourages Users from utilizing browser bookmarks with the HDT application.

## 4. GETTING STARTED

This section explains the HDT application from initiation through exit.

## 4.1. Set-up Considerations

The CMS Enterprise Portal supports the following internet browsers:

- Mozilla Firefox
- Chrome
- Safari

CMS recommends the Chrome internet browser for HDT Users.

HDT Users should follow the login process outlined in <u>Section 4.3.6</u> of this User Guide. Users should manually enter all internet addresses (Uniform Resource Locators, or URLs) into your internet browsers. CMS discourages Users from utilizing browser bookmarks with the HDT application.

To optimize access to the HDT application, please disable pop-up blockers prior to use.

CMS discourages HDT Users from utilizing Auto-fill or Auto-populate features of internet browsers. Users should disable these features in their browsers when using HDT.

HDT Users should make adjustments to 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 of time. Because the HDT application framework has been developed to use similar page components, it is important that the user's browser is set to ensure that it tries to locate and retrieve a fresh instance of the HDT page and the data content.

HDT Users should enable JavaScript and adjust any zoom features to ensure you are not seeing the screen in too wide of a view.

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

## 4.1.2. Google Chrome

CMS discourages the use of autofill features. To remove the autofill feature in Google Chrome, perform the following:

- 1. Go to [Settings]
- 2. Select [Show advanced settings...]
- 3. Under the [Passwords and forms] sections, make sure the box next to [Enable Autofill to fill out web forms in a single click] is not checked.

## 4.2. User Access Considerations

Clearinghouse and Direct Provider Submitters must be granted permission to access the HDT application. Users must have an active, valid HETS 270/271 Submitter ID.

HDT Users must have a CMS Enterprise Portal User ID that is 32 characters or less to utilize the HDT application. The HDT application also requires that CMS Enterprise Portal User IDs and User first and last names only contain standard characters. Special characters such as apostrophe (' ' ') and hyphen (' - ') are not compatible with HDT. CMS Enterprise Portal Users who request the HDT role for an existing CMS Enterprise Portal User ID that is greater than 32 characters and/or contains any special characters in the User ID or User first or last names will not be granted access to the HDT application.

## 4.3. Accessing the HDT Application

The HDT application is accessible to Submitters through the CMS Enterprise Portal. Approved CMS Enterprise Portal Users must add the HDT role to their profile from the CMS Portal Access Catalog then obtain CMS approval before HDT access will be granted.

### 4.3.1. Requesting HDT Access for an Existing CMS Enterprise Portal Account

If you have an approved, established CMS Enterprise Portal account, you must submit a request to add the HDT role to your existing profile.

<u>Note</u>: CMS Enterprise Portal Users that add the HDT User role may be required to complete the Remote Identity Proofing (RIDP) process. As part of RIDP, the system will require answers to questions related to your personal and financial information. So, please have your personal and credit information handy prior to attempting RIDP.

1. Navigate to <u>https://portal.cms.gov/</u>. The *CMS Enterprise Portal* page is displayed, as illustrated in Figure 1.

CMS.gov Enterprise Portal		Hind Your Application	? Help	(i) About	🖂 E-mail Alerts
	CMS.gov Enterprise Por	tal	(	21	7
	UserID	- 17			
	Password	- 14			
The THEFT	Agree to our <u>Terms &amp; Conditions</u>	_ <			1
	Login Forgot your <u>User ID</u> or your <u>Password</u> ?				
	rongor your <u>user in</u> or your <u>rassworu</u> :	_			
	New User Registration				
		~			
	About				

## Figure 1: CMS Enterprise Portal Login Screen

- 2. Enter your CMS Enterprise Portal User ID in the User ID field.
- 3. Enter your CMS Enterprise Portal password in the **Password** field.

4. CMS Enterprise Portal Users whose accounts have already been escalated will be required to enter their Multi-Factor Authentication (MFA) credentials, selecting an MFA Device that has already been associated with the CMS Enterprise Portal User ID, and then entering the appropriate Security Code from that device (see Figure 2). Select the [MFA Device Type] you wish to use from the drop-down menu and then enter the Security Code (VIP Token) you obtained, check the [I Agree to our Terms and Conditions] if you agree, then select [Log In]. If the Users account has not already escalated to require MFA authentication, then the User will only need to enter their CMS Enterprise Portal password. Enter the **Password** and any required MFA information, check the [I Agree to our Terms and Conditions] if you agree, then [Log In].

#### Figure 2: CMS Enterprise Portal Login Screen with Multi-Factor Authentication

CMS.gov Enterprise Portal	E Find You	ar Application ③ Help	About E-mail Alerts
	CMS.gov Enterprise Portal		AV
	DEV_TEST20		
P-	•••••	100	
	Text Message (SMS)	100	
11-14	MFA Code Sent 409964		
	The Security code for the Text Message (SMS) will expire in 10 minutes.		
	Trouble Accessing Security Code?		
Constant ( 1970)	Agree to our Terms & Conditions           Login		
	Forgot your <u>User ID</u> or your <u>Password</u> ?		

#### Notes:

- If you need to register a MFA Device, select the [Register MFA Device] link and complete the process described in <u>Section 4.3.4.1.</u>
- If you have registered a MFA Device but are temporarily unable to access that device, you may utilize the [Unable to Access Security Code] link. See <u>Section 4.3.4.2</u> for complete details on using this feature.
- If you enter your CMS Enterprise Portal password incorrectly three times, the system will lock your account. While your account is locked, you cannot access any other features. You must contact the MCARE Help Desk to reset your CMS Enterprise Portal password as described in <u>Section 6.5</u>.

- When an Administrator resets your CMS Enterprise Portal password, you
  will be sent an email with a temporary one-time password. You must then
  login to the CMS Enterprise Portal and change the password to one of
  your choice, following the CMS & HDT Password Policy. Please note that
  HDT requires that CMS Enterprise Portal passwords contain only
  alphanumeric characters. Refer to <u>Section 4.3.3.3</u> of this document for
  instructions on changing your password.
- 5. After logging in, the **My Apps** page is displayed, as illustrated in Figure 3. Select the [Request/Add Apps icon] that appears under My Apps. Alternately, you may select [down arrow icon] that appears next to your name at the top of the page to continue.

C	MS.gov My Enterprise Portal	Welcome TESTACCOUNT ABEL -	Help	🕞 Log Out
	My Apps			
	You currently do not have access to any CMS applications. Please request acces	s below.		
	Request/Add Apps			

#### Figure 3: My Access Screen

6. The [Access Catalog], [My Access] and [My Pending Requests] sections are displayed, as illustrated in Figure 4. Scroll down to locate the application you need, if it is not displayed. Alternatively, enter the first few letters of the application in the [Search] section and all of the applications beginning with those letters will be displayed. <u>Note</u>: If you currently have access to one or more applications, those applications are displayed in the [My Access] section. If you have pending requests, they are displayed in the [My Pending Requests] section.

## Figure 4: My Access Screen

CMS.gov My E	nterprise Portal	🔳 My Aj	pps	Welcome Arpitha Pereyala 🔻	? Help	🕩 Log Ou
ccess Catalog Star	t typing to filter apps		My Access			
			FFSDCS	Available Actions		
adasdasd asdasdas Help Desk Information 123123123123 asdasdasd	AlFtest aplication(@#\$%*(ol) -(Ik+cSecfs?(s)fs[sad] test application modify(@#5%*(ol);#k- test application modify(@#5%*(ol);#k- Help Desk Information 123-456-7800(@#5%*(ol);#k- SampleTESI@pseinc.com/@#5%*(ol) (s)fs[ad]	Help Desk Information 12312312 <u>aasasda</u>	Help Dask Information 123-456-7800 Samulet TEST Øgssine.com Existing Roles ASP PEnd User ASP Helpdesk User ASP Staff	Add Role Remove Role Other Actions		
Request Access	Request Access	Request Access	Comprehensive Primary Care Initiative (CPC)	Available Actions Add Role		
asdasdas asdasdasdas	ASETT ASETT is a Web-based application t individuals and organizat Mor	asfail prov1 hat allows werewr	Help Desk Information 123-456-7890 SampleTEST@qssinc.com	Remove Role Other Actions		
Help Desk Information 12312313123 <u>sadasdas</u>	Help Desk Information 123-456-7890 Sample TEST @gssinc.com	Help Desk Information sdisdridf <u>dsfsdfsdf</u>	Existing Roles CPC Basic User			
Request Access	Request Access	Request Access	Connexion Help Desk Information 123-456-7890 Sample TEST@qssinc.com Existing Roles	Aveilable Actions Add Role Remove Role Other Actions		
asfail prov1 sfsdfsdf	BCRS Web The Benefits Coordination & Recove (BCRS) allows a user t More	ry System Bundled Payments For Care Improvement Data File Transfer.	Connexion CBIC-Input			
Help Desk Information sdfsdf asfsdf	Help Desk Information 123-456-7890 SampleTEST@qssinc.com	Help Desk Information 123-456-7890 SampleTEST@qssinc.com	EIDM Help Desk Information 123-456-7890 SampleTEST@qssinc.com	Available Actions Add Role Remove Role Other Actions		
Request Access	Request Access	Request Access	Existing Roles EIDM Helpdesk Tier 1			
CBIC-DEMO Connexion - Competitive Bidding Imple Carrier (CBIC) Web Port More,	The CCIIO Enrollment Resolution	n and The CMS WebEx cloud offering consists of access to WebEx Training Cent More	Eligibility and Enrollment Medicare Online (ELMO) Help Desk Information	Available Actions Add Role Remove Role		
Help Desk Information	Reconciliation System (CERRS) sup	P More Help Desk Information	123-456-7890 SampleTEST@gssinc.com	Other Actions		

 After entering the first few letters of the application in [Search], the applications beginning with those letters are displayed, as illustrated in Figure 5. Select [Request Access] for the HETS Desktop (HDT) role.

#### Figure 5: Request Access

CMS.gov My Enterprise Portal				Welcome 🔻 Beta	aVal ValBeta	Help	E Log Out
Access Catalog hdt	REQUEST ADMIN ROLE	SHOW ALL	My Access				
HDT HIPA-Eligibity Transaction System (HETS) Desktop Help Desk Information 123-45-780 ServerkhPL-Destant.com			You currently do not have access to any appl access catalog to request access to the appl	ications. Please use the cations.			
			My Pending Requests You do not have any pending requests at this	s time.			

8. The Application Description and Select a role sections are displayed, as illustrated in Figure 6. Select the HDT User role from the [Select a Role] drop down menu.

## Figure 6: Select a Role

·	My Enterprise Portal Welcome 🔻 BetaVal ValBeta	? Help	🕩 Log Out
My Access View and Manage My	Request New Application Access * Required Field		iHelp
Request New Application	Application Description: HDT		et a Role
cess Requests	HIPAA Eligibility Transaction System (HETS) Desktop		rom the options beir splayed.
Annual Certification My Pending Requests	Select a Role: [HDT User   Role Description: The user with this role is a staff member who is trusted to perform Medicare business for the application. HPG User with a Submitter ID is associated with a Gentran mailbox.		
	This role requires Identity Verification and may require multi-factor authentication credentials to be set up. If your Level of Assurance has not been met for this role, you will be asked to provide additional information to verify your identity and if applicable, register a device for multi-factor authentication. Please select 'Next' to continue		
	Next Cancel		

The page indicates that the selected HDT User role requires Identity Verification, as illustrated in Figure 7. Select [Next] to continue.

Figure 7: HDT User Role Identity Verification

CMS.gov	My Enterprise Portal	Welcome 🔻 BetaVal ValBeta	Help	🕞 Log Out
My Access	Request New Application Access	* Required Field		iHelp
Access Request New Application Access	Application Description: (HDT HDPAA Eligibility Transaction System (HETS) Desktop		Select a value	ect a Role from the options being displayed.
	Select a Role: [HDT User  Role Description: The user with this role is a staff member who is trusted to perform Medicare business for the application. HPG User with a Submitter II This role requires Identity Verification and may require multi-factor authentication credentials to be set up. If your Level of Assurance to provide additional information to verify your identity and if applicable, register a device for multi-factor authentication. Please select	as not been met for this role, you will be asked		

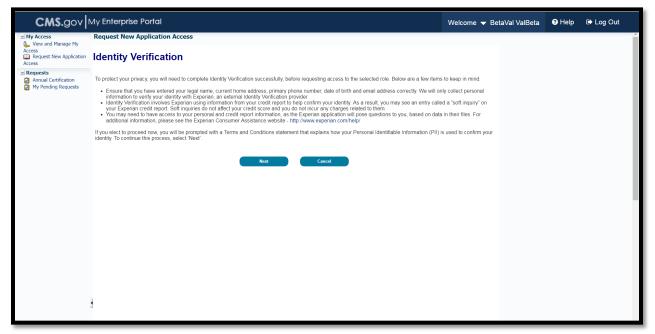
9. Depending on your CMS Enterprise Portal account, you may now be directed to the *Identify Verification* page, as illustrated in Figure 8. This identify verification process (Remote Identity Proofing or RIDP) is used to verify your identity and is done by asking questions based on your personal and credit report information.

If you are not required to complete the RIDP process, please proceed to Step 14.

<u>Note</u>: You have ten (10) minutes to complete RIDP. Otherwise you will lose all of the information you entered and will need to start the process again.

Select [Next] to begin the Identify Verification section.

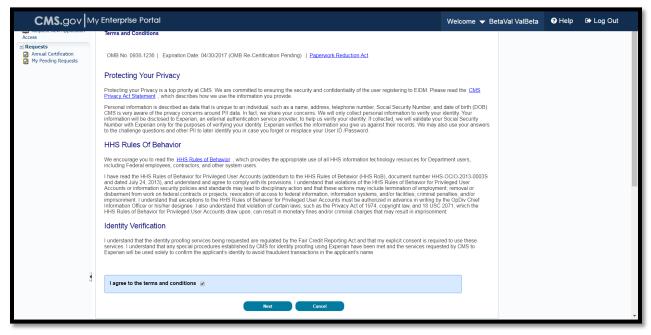
### Figure 8: Identity Verification Screen



10. Read the *Terms and Conditions*, as illustrated in Figure 9. Select the [I agree to the terms and conditions] checkbox and then select [Next].

<u>Note</u>: [Next] will be enabled only after checking the [I agree to the terms and conditions] checkbox.

Figure 9: Terms and Conditions Screen



11. Confirm your email address and enter your Social Security Number (Social Security Number is optional when creating the user ID but is required when applying for HDT), as illustrated in Figure 10. Verify the pre-populated information then select [Next] to continue the identity verification process.

CMS.gov	Ay Enterprise Portal	Welcome 👻 BetaVal ValBeta	Help	🕩 Log Out
Y Access     Wre and Hange My     View And Hange My     Access     We construct the Application     Access     Request     Access     My Pending Requests	Request New Application Access         Your Information         Enter your legal first name and last name, as it may be required for Identity Verification.         • First Name         BetaVal         • Last Name         Suffic         ValBeta         • Enter your E-mail address, as it will be used for account related communications.         • Enter your E-mail address,         • Confirm E-mail Address.         • Confirm E-mail Address         Enter your thill 0 digit Social Security Number, as it may be required for Identity Verification.         • Social Security Number:         • Enter your date of birth in MMNDD/YYYY format, as it may be required for Identity Verification.         • Date of Birth:			
	10       17       1970         10       17       1970         10       17       1970         10       17       1970         10       17       1970         10       17       1970         10       17       1970         10       17       1970         11       betavisy       1         11       betavisy       1         Home Address Line 1:       1         11       betavisy       1         Home Address Line 2:       1         • Cdy       • State       • Zp Code         Betatoan       Country: USA         Enter your primary phone number, as it may be required for identity Verification.       • Primary Phone Number         800       676       1234			

### Figure 10: Your Information Screen

12. Provide an answer to each question in the *Verify Identity* section, as illustrated in Figure 11. Select [Next] to continue. If you wish to terminate the request, select the [Cancel] button and you will be returned to the View and Manage My Access page.

<u>Note</u>: Verify Identity questions are provided from Experian based on the information provided in Step 11.

## Figure 11: Verify Identity

Your Information Verify Your Identity
Verify Identity
You may have opened a mortgage loan in or around August 2012. Please select the lender to whom you currently make your mortgage payments. If you do not have a mortgage, select 'NONE OF THE ABOVE/DOES NOT APPLY.
O NORVEST BANK
C PARKWAY MTG
O NONE OF THE ABOV BODES NOT APPLY
Which of the following is a current or previous employer? If there is not a matched employer name, please select 'NONE OF THE ABOVE'.
© DRP CONS
C ENGR CUSTOM PLASTIC
SOUTH JERSEY GAS CO
US MARNES
O NONE OF THE ABOV EDDES NOT APPLY
According to our records, you previously lived on (7TH). Please choose the city from the following list where this street is located.
© VIRGINA
© CHISHOLM
© WINONA
© GRAND RAPIDS
O NONE OF THE ABOV EDDES NOT APPLY
Please select the number of bedrooms in your home from the following choices. If the number of bedrooms in your home is not one of the choices please select 'NONE OF THE ABOVE'.
0 2
0 3
0 4
0 5
NONE OF THE ABOV EDDES NOT APPLY
Please select the county for the address you provided.
O BERGEN
© CAMDEN
© AT LANTIC
© MORRIS
NONE OF THE ABOV BDDES NOT APPLY  Ne xt  Cancel

13. If the Verify Identity questions were answered properly, the Remote Identify Proofing (RIDP) process is now complete. Select [Next] to continue with the HDT User role request process, as illustrated in Figure 12.

<u>Note</u>: If you encounter any issues with the RIDP process, please refer to <u>Section 4.3.5</u> for additional information including support options.

<u>Note</u>: If the CMS Enterprise Portal directs you to complete the Multi-Factor Authentication (MFA) registration process now, then please refer to <u>Section 4.3.4</u> for instructions.

## Figure 12: Complete Set Up



After completing Your Information, the Multi-Factor Authentication Information page is displayed, as illustrated in Figure 13. Click [Next] to begin the MFA Registration process.

Figure 13: Multi-Factor Information Screen

CMS.gov	My Enterprise Portal	Welcome 🔻 BetaVal ValBeta	? Help	🕩 Log Out
My Access	Request New Application Access			Î
Access	Multi-Factor Authentication Information			
✓ Requests Annual Certification My Pending Requests	To protect your privacy, you will need to add an additional level of security to your account. This will entail auccessfully registering your Phone, Comp continuing the role request process. To continue this process, please select 'Next'. <u>Next</u> <u>Cancel</u>	uter or E-mail, before		

 Read the *Register Your Phone, Computer or Email* page notification, as illustrated in Figure 14. Review the available options and determine which option(s) you will use for MFA. Note that a CMS Enterprise Portal can register multiple MFA options (i.e., phone, laptop and text messaging). If necessary, download and install any software or applications necessary to that MFA option. When complete, select an option from the [Credential Type] dropdown menu.

<u>Note</u>: Regardless of the mechanism you choose, when using MFA, you will have a limited time to retrieve and enter the MFA security code. If you are unable to enter the MFA security code within that limited time, then the code will expire and you will need to request a new security code.



CMS.gov	My Enterprise Portal	Welcome 👻 BetaVal ValBeta	Help	🕩 Log Out
My Access	Request New Application Access			^
Access Request New Application Access	Register Your Phone, Computer, or E-mail			
Requests     Annual Certification     My Pending Requests	Adding a Security Code to your login also known as Multi-Factor Authentication (MFA) can make your login more secure by providing an extra layer of user name and password. You can associate the Security Code to your profile by registering your Phone, Computer or E-mail. Select the links below to find out more information	about the options.		
	Select the MFA Device Type that you want to use to login to secure applications from the dropdown menu below.  MFA Device Type Priore/TabletPCLaeto  Credential ID : VSST44379221  MFA Device Description: VIP  Rect Cance			

After selecting your Multi-Factor Device Type, Select [Next] to continue.

2. Your registration for Multi-Factor Authentication is now complete. Select [Next] to continue, as illustrated in Figure 15.

<u>Note</u>: You will receive an email notification for successfully registering the MFA credential type.

Figure 15: Complete Set Up

CMS.gov	My Enterprise Portal	Welcome 🔻 BetaVal ValBeta	Help	🗈 Log Out
My Access     View and Manage My     Access     Request New Application     Access     Mr Access     Mr Access     Mr Acquests     Mr Acquests     Mr Pending Requests	Request New Application Access Register Your Phone, Computer, or E-mail You have successfully registered your Phone/Computer/E-mail to your user profile. Please select: Next to continue with your role request.  Text			

3. After completing the Multi-Factor Registration process, *Request New Application* page is displayed, as illustrated in Figure 16. If all of your required business contact information is not on file, you will have to provide this information before you can continue. Required fields are marked with an asterisk (\*) and an error message will be displayed, if the information has not been entered, selected correctly, or entered in the correct format.

<u>Note</u>: If all of your business contact information is on file, the "Please update your profile..." message will not be displayed and the "Select a role" drop down menu will be displayed for you to continue. (See Step 11.) If the "Please update your profile..." message is displayed, enter the required information and then select [Next].

#### Figure 16: Request New Application Access Screen

			🕩 Log Out
Request New Application Access * Required Field			iHelp
Please update your profile to continue the request for an application access.		Enter an Office you can be o	Phone Number where
Title:    First Name: BetaVal Middle Name: Last Name: ValBeta Suffix:   Professional Credentials:  Social Security Number:  *******1234  Business Contact Information * Company Name: MCARE VAL TESTING * Address 2:		Please enter th following for	e phone number in the mat: 300-3000-3000.
* Stat/Terrory (Ealfornia v * Zip Code: 90210 Zip Code Extension: Phone			
* Company Phone Number: 800-345-7891 Extension: * Office Phone Number: 800-345-1978 Extension:	Next Cancel		
	Hease update your profile to continue the request for an application access.         Name         Title: <ul> <li>First Name:</li> <li>BetaVal</li> <li>Middle Name:</li> <li>Last Name:</li> <li>ValBeta</li> <li>Suffix:</li> <li>Suffix:</li> <li>Forst Summer MCARE VAL TESTING</li> <li>* Address 2:</li> <li>* Company Name:</li> <li>* Clark:</li> <li>EVATOR</li> <li>* StateTTentory, California</li> <li>* Zip Code:</li> <li>90210</li> <li>Zip Code Extension:</li> <li>Phone</li> <li>* Company Phone Number:</li> <li>500-345-7891</li> <li>Extension:</li> <li>Extension</li></ul>	Hease update your profile to continue the request for an application access.     Name     Title:     First Name:     BetaVal        Middle Name:     Last Name:        Sufface:     Social Security Number:     * Company Name:     * Address 2:        * Company Name:     * Company Phone Number:     * Office Phone Number:	* Required Field     Office P       reters an Office of an application access.     The image of the application access.       Name     The image of the application access.       Title:     First Name:     Middle Name:     Last Name:       Value     Middle Name:     Last Name:     Valueta       Social Security Number:     ************************************

 After providing your business contact information, the CMS Enterprise Portal will ask you to provide your RACF ID (if applicable), your organization's HETS 270/271 Submitter ID, and your reason for the request in the [Reason for Request] box, as illustrated in Figure 17. Then select [Next].

#### Figure 17: Provide RACF ID, Submitter ID, and Reason for Request

My Enterprise Portal	Welcome 🔻 BetaVal ValBeta	? Help 🕞 Log Out
Request New Application Access	* Required Field	iHelp
Application Description: [HDT v HIPAA Eligibility Transaction System (HETS) Desktop		Reason for Request The 'Reason for Request' field represents the justification for
Select a Role: HDT User		submitting the request and can contain any additional comments.
Role Description: The user with this role is a start memoer who is trusted to perform medicate business for the application. This user with a submitte RACF ID: Submitter ID: B1231456	r 1D is associated with a Gentran maildox.	
Reason for Request: Used for testing		
Å	Next Cancel	
	Request New Application Access         Application Description:         HIPAA Eligibility Transaction System (HETS) Desktop         Select a Role:       HDT user         Role Description:       The user with this role is a staff member who is trusted to perform Medicare business for the application. HPG User with a Submitter         RACF ID:	Request New Application Access       * Required Field         Application Description:       HDT         HIPAA Eligibility Transaction System (HETS) Desktop         Select a Role (HDT User         Role Description:         Role Description:         RACF ID:         Submitter ID:         Submitter ID:         B1237456

 After selecting [Next], the *Request New Application Access Review* page is displayed, as illustrated in Figure 18. Review the information displayed. Select [Edit] to modify the information. Select [Submit] to submit the request for approval.

<u>Note</u>: You may select [Cancel] to exit out of the Request New Application Access process. All information provided, and any changes made, will not be saved. In the example below, the information is correct. Select [Submit] to submit the request for approval.

#### Figure 18: Request New Application Access Review

CMS.gov	My Enterprise Portal	Welcome 👻 BetaVal ValBeta	③ Help
Access Request New Application Access	Application Description: HDT v HIPAA Eligibility Transaction System (HETS) Desktop	Requires ries	Review The Review page allows you to review your request. Please select an action
Requests     Annual Certification     My Pending Requests	Role Selected: HDT User Role Description: The user with this role is a staff member who is trusted to perform Medicare business for the application. HPG User with a Submitte	r ID is associated with a Gentran mailbox.	to continue.
	Name Title:  First Name: BetaVal Middle Name: Last Name: ValBeta Suffix:  Professional Credentials: Social Security Number:  *******1234		
	Business Contact Information Company Name: MCARE VAL TESTING Address 1: 1224 TEST ST Address 2: CRV: BETATOWN State/Territor: Claffornia Zip Code: 190210 Zip Code Extension:		
	Company Phone Number:         800-345-7891         Extension:           Office Phone Number:         800-345-1978         Extension:		
	RACF ID: B1237456		
	Reason for Request: Used for testing	Edit Submit Cancel	

6. After selecting [Submit], the *Request New Application Access Acknowledgement* page is displayed, as illustrated in Figure 19. The acknowledgement page displays the tracking number for the request and informs you that you will receive an email when the request has been processed.

Select [OK] to close the acknowledgment page.

#### Figure 19: Request New Application Access Acknowledgement

CMS.gov	My Enterprise Portal	Welcome 🔻 BetaVal ValBeta	Help	🗈 Log Out
✓ My Access     View and Manage My     Access     Q     Request New Application     Access	Request New Application Access Acknowledgement Your EIDM request has been successfully submitted. The tracking number for your request is: 2609872 - ADD - HDT User		Ackno Your request	iHelp wledgement or requests have been ubmitted.
<ul> <li>✓ Requests</li> <li>Annual Certification</li> <li>My Pending Requests</li> </ul>	Please use this number in all correspondence concerning this request. You will receive an email once your request has been processed.	( ОК )		

### 4.3.2. CMS Enterprise Portal New User Registration

If you do not have an approved, established CMS Enterprise Portal account, you must create a new CMS Enterprise Portal account and then request to add the HDT role to that new profile. The CMS Enterprise Portal is available at <a href="https://portal.cms.gov/wps/portal/unauthportal/home/">https://portal.cms.gov/wps/portal/unauthportal/home/</a>.

<u>Note:</u> The CMS Enterprise Portal will require you to verify your identity to gain HDT access. Please provide personal information such as Name, Date of Birth, Address, etc. as recorded in either your driver's license or any Government ID.

<u>Note:</u> HDT requires that all CMS Enterprise Portal User IDs be 32 characters or less (see <u>Section 4.2</u>). The HDT application also requires that CMS Enterprise Portal User IDs and User first and last names only contain standard characters. Special characters such as apostrophe (''') and hyphen ('-') are not compatible with HDT. Please keep these constraints in mind as you create your CMS Enterprise Portal account User ID and enter your name into the CMS Enterprise Portal.

1. Navigate to <u>https://portal.cms.gov</u>. The *CMS Enterprise Portal* page is displayed, as illustrated in Figure 20.

CMS.gov Enterprise Portal	=	Find Your Application	🕑 Help	1 About	🖂 E-mail Alerts
	<b>CMS</b> .gov Enterprise Portal		1	2	7
	UserID Password	- 7			
	Agree to our <u>Terms &amp; Conditions</u>	- 2			1
	Login Forgot your <u>User ID</u> or your <u>Password</u> ?				
	New User Registration				7
	About				

## Figure 20: CMS Enterprise Portal Screen

2. Select [New User Registration], as illustrated in Figure 21.

#### Figure 21: New User Registration

CMS.gov Enterprise Portal	🖶 Find Your Application	🕜 Help	1 About	🖂 E-mail Alerts
	CMS.gov Enterprise Portal	(	21	1
	UserID			
	Password Agree to our <u>Terms &amp; Conditions</u>			1
	Login Forgot your <u>User ID</u> or your <u>Password</u> ?			
				7
	New User Registration			

3. Select your application under the [Choose your Application] drop down. Then, as illustrated in Figure 22.

Figure 22: Choose your Application

CN	AS.gov Enterprise Portal	Find Your Application	? Help	i About	🖂 E-mail Alerts	
	Step #1: Choose Your Application					
	Step 1 of 3 - Select your application from the dropdown. You will then need to agree to the terms					
	Choose Your Application				~	

Upon agreeing to the terms and conditions, Click Next. See Figure 23.

### Figure 23: Terms and Conditions

CMS.gov Enterprise Portal		🗱 Applications 😯 Help 🚯 About 🔤 E-Mail Alerts
	Step #1: Choose Your Application         Step 1:01-Stelet.your application from the dropdown. You will then need to agree to the terms.         HOT(NPG:: HIMA Eligibility Transaction System (HETS) Desktop	
	Terms & Conditions ONE to 0351/205[ Everation Date: 03/31/2021   Paperwork Reductor Act Consent to Monitoring Polyogray on the weblek, you consert to be monitored. Unauthorized attempts to upload information and/or change information on this web site are strictly prohibite and are subject to procession under the Computer Fraud and Abuse Act of 1968 and Title 10. U.S. C. Sec. 1001 and 1030. We encourage you to read webles attempts to the strictly and the strictl	
	✓ I agree to the terms and conditions Next Cancel	

4. The Register Your Information page is displayed, as illustrated in Figure 24. Provide the information requested on the Register Your Information page. All fields are required unless marked "Optional". After all required information has been provided, select [Next] to continue.

<u>Note</u>: You may select [Cancel] at any time to exit out of the User ID registration process. All information provided, and any changes made, will not be saved.

#### **Figure 24: Register Your Information**

CMS.gov Enterprise Portal	Hind Your Application	? Help	i About	🖂 E-mail Alerts
Store Ho. Devictor Very Information				
Step #2: Register Your Information				
Step 2 of 3 - Please enter your personal and contact information.				
All fields are required unless marked 'Optional'.				
Enter First Name Enter Middle Name (optional) Enter Las	st Name	Suffix (opti	onal)	•
Enter Social Security Number (optional) Birth Month 🔻 Birth Date	Birth Year	•		
Is Your Address US Based?				
Enter Home Address #1 Enter Ho	me Address #2 (optional)			
Enter City State The Enter Zip	Code	Enter Zip+	+4 (optional)	
Enter E-mail Address Confirm E-mail Addres	ss			
Enter Phone Number				
Back Next Cancel				

5. After providing the required information on the Register Your Information page, the Create User ID, Password & Security page is displayed, as illustrated in Figure 25. Create and enter a [User ID] of your choice and based on the requirements for creating a User ID.

<u>Note</u>: The CMS Enterprise Portal will display instructions on what you are required to include in your User ID.

<u>Note</u>: Please note that HDT requires that all CMS Enterprise Portal User IDs be 32 characters or less. The HDT application also requires that CMS Enterprise Portal User IDs and User first and last names only contain standard characters. Special characters such as apostrophe (' ' ') and hyphen (' - ') are not compatible with HDT (see <u>Section 4.2</u>).

#### Figure 25: Choose User ID and Password

CMS.gov Enterprise Portal		📕 Find Your Application	? Help (1) Abo	out 🖂 E-mail Alerts
Step #3: Create User	ID, Password & Sec	urity		
Step 3 of 3 - Please create User ID and P	bassword, Select security questions and	provide answers.		
Enter User ID				
Enter Password	Enter Confirm Password			
Select Security Question #1	•	Enter Security Question #1 Answer		
Select Security Question #2	•	Enter Security Question #2 Answer		
Select Security Question #3	•	Enter Security Question #3 Answer		
Back	lext Cancel			

6. Create and enter a password of your choice, as illustrated in Figure 24

<u>Note</u>: The CMS Enterprise Portal will display instructions on what you are required to include in your password. Enter the same password for "Confirm Password".

Note: The passwords must match before you can continue.

7. After entering a user created User ID and password, select a question of your choice in the [Select your Challenge Questions and Answers] section and then enter the answer you want to be saved with the question. . Continue to select a question and to enter an answer for Question 2 and Question 3. Select [Next] to complete the registration process.

<u>Note</u>: You may select Cancel to exit out of the User ID registration process. All information provided, and any changes made, will not be saved. In the example below, select Next to complete the registration process.

<u>Note</u>: The questions displayed on the actual Choose User ID and Password page may be different than the questions displayed in this user manual.

8. After selecting [Next], the *Registration Summary* page is displayed, as illustrated in Figure 26. The *Registration Summary* allows you to review the

information entered for accuracy before submitting. Select [Submit User] to submit your registration request once reviewed.

Figure	26:	Registration	Summary
--------	-----	--------------	---------

CMS.gov Enterprise Portal							Applications	Help     About	E-Mail Alerts
	Registration Sun	nmary							
	Please review your information and ma	ake any necessary changes befor	e submittin	ng.					
	HOUSE FIRST Eighting Transition					~			
	All fields are required unless marked								
	First Name BetaVal	Hiddle Name (optional) V		Last Name ValBeta	Suffix (optional)	~			
	Social Security Number (optional) 012345678	Birth Month May	*	Sinth Date Sinth Year 31 ¥ 1980	~				
	Home Address #1 MCARE VAL TESTING			Home Address #2 (optional) 1234 TEST ST					
	City BETATOWN	State California	~	Zip Code 90210	Enter Zip+4 (optional)				
	E-mail Address VALTESTING@MCARE.COM		Confirm	I E-mail Address IG@MCARE.COM					
	Phone Number 800-012-3456								
	User 10 WALTESTID								
	Password	Confirm Password	۲						
	What is your favorite radio station?		*	Challenge Question #1 Answer 1.0.2					
	What is the name of your favorite pet?		•	Challenge Question #2 Answer spot					
	What is your parents' wedding anniversary	y date?	*	Challenge Question #3 Answer 01012001					
	Submit User	Cancel							
	Centers for Medicare	nent website managed by the U e & Medicaid Services. 7500 Sec ird, Baltimore, MD 21244	l.s. curity		💌 👌 🕅				Тор

9. After selecting [Submit User], the Confirmation page is displayed, as illustrated in Figure 27. The Confirmation page informs you that you will receive an email acknowledging your successful registration and will include your User ID. Select the [X] to close the *Confirmation* page.

### Figure 27: Confirmation

CMS.gov Enterprise Pr	ortal	Find Your Application	Help	i About	🖂 E-mail Alerts	
	♥Confirmation		×			
	Your ID has been successfully registered with CMS Enterprise Portal. An e-mail has been sent to your registered e-mail address here.	s.You can now login by clickii	ıg			

10. After creating your CMS Enterprise Portal User ID and password, follow the steps outlined in <u>Section 4.3.1</u> to add the HDT User role to your profile.

#### 4.3.3. CMS Enterprise Portal User ID and Password Management

CMS Enterprise Portal User IDs and passwords are assigned to individuals. Individuals are strictly forbidden from sharing their CMS Enterprise Portal User IDs and passwords with others. The unauthorized use of an individual's CMS Enterprise Portal User ID and password will result in the termination of that CMS Enterprise Portal User ID and password.

#### 4.3.3.1. Forgotten CMS Enterprise Portal User ID

If you have forgotten your CMS Enterprise Portal User ID, refer to Section 5 of the EIDM/CMS Enterprise Portal User Guide for complete instructions on how to resolve that issue. A link to the EIDM/CMS Enterprise Portal User Guide is available in <u>Section 2</u> of this document.

#### 4.3.3.2. Forgotten CMS Enterprise Portal Password

If you have forgotten your CMS Enterprise Portal password, refer to Section 5 of the EIDM/CMS Enterprise Portal User Guide for complete instructions on how to resolve that issue. A link to the EIDM/CMS Enterprise Portal User Guide is available in <u>Section 2</u> of this document.

#### 4.3.3.3. Changing Your CMS Enterprise Portal Password

If you choose to or are required to change your CMS Enterprise Portal password, refer to Section 5 of the EIDM/CMS Enterprise Portal User Guide for complete instructions on how to accomplish that task. A link to the EIDM/CMS Enterprise Portal User Guide is available in <u>Section 2</u> of this document.

#### 4.3.4. Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is a security mechanism that is implemented to verify the legitimacy of a person or transaction.

MFA is an approach to security authentication which requires users to provide more than one form of verification in order to prove their identity. MFA registration is required only once, but will be verified every time you log into the CMS Enterprise Portal.

Additional details about MFA are available in the HETS RIDP & MFA FAQs available in <u>Section 2</u> of this document.

#### 4.3.4.1. Registering for Multi-Factor Authentication (MFA)

Registered CMS Enterprise Portal Users with an existing account who wish to access a CMS MFA protected application (like HDT) will be directed through the MFA registration process.

During the MFA registration process, the CMS Enterprise Portal requires registration of a phone, computer or email to add an additional level of security to a User's account. The User is given five options to select from to complete the registration process. The same steps can be followed to register multiple MFA devices.

Depending on the MFA option you choose to register, you may need access to download and install software on your computer or phone; your phone should be able to receive text messaging (SMS); or you should have a valid email address.

HDT Users who wish to complete their MFA registration prior to signing into the HDT system can follow these steps.

1. Navigate to <u>https://portal.cms.gov/</u>. The *CMS Enterprise Portal* page is displayed, as illustrated in Figure 28.

CMS.gov Enterprise Portal		Eind Your Application	? Help	<ol> <li>About</li> </ol>	🖂 E-mail Alerts
	<b>CMS.</b> gov Enterprise Po	rtal	(	20	7
	UserID				
	Password	_			
- 1/2 DEPT	Agree to our <u>Terms &amp; Conditions</u>	_ /			1
	<b>Login</b> Forgot your <u>User ID</u> or your <u>Password</u> ?				-
	New User Registration				

#### Figure 28: CMS Enterprise Portal Screen

2. Enter your CMS Enterprise Portal User ID and Password, Click the [Agree to our Terms and Conditions] to continue the Registration process, then Login, as illustrated in Figure 29.

CMS.gov Enterprise Portal		Eind Your Application	🕜 Help	(i) About	⊠ E-mail Alerts
			0	51	1
	CMS.gov Enterprise Port	tal			
	UserID	- 7			
	Password Agree to our <u>Terms &amp; Conditions</u>				1
	Login				
	Forgot your <u>User ID</u> or your <u>Password</u> ?				
	New User Registration				
13	C. Part C. C.				

#### Figure 29: Login to CMS Enterprise Portal

3. Select your username and then select [My Profile] from the dropdown menu to go to your profile, as illustrated in Figure 30.

## Figure 30: Select My Profile

S.gov My Enterprise Portal		Welcome TESTACCOUNT ABEL 🗕 🕜 Help 🕞 Lo
		My Access My Profile
My Profile Manage Profile	View My Profile	Change My Profile
View Profile	First Name: TESTACCOUNT	
Change Profile	Last Name:	
Change Password	Middle Name:	
Change Security Questions	Date of Birth:	
Register MFA	E-mail Address:	
Remove MFA	Phone Number:	
	Home Address Line 1:	
	Home Address Line 2:	
	City: Baltimore	
	State: MD	
	<b>Zip Code:</b> 21244	
	Country: USA	

4. Select [Register MFA] from the navigation links on the left to begin the process of adding MFA to your account, as illustrated in Figure 31.

#### Figure 31: Register MFA

My Profile		
Manage Profile	Register Your MFA Device (Phone, Computer	or E-mail)
View Profile	Adding a Security Code to your login, also known as Multi-Factor Authentication (MFA), can make your login more secure by providing an extra layer of protection to your user name and password. Click here to learn more about MFA and or go ahead and register your device. Select the MFA device type that you want to use to login	
Change Profile		
Change Password		
Change Security Questions	Choose MFA Device	w.
Register MFA	Submit Cancel	
Remove MFA.		

5. Read the *Register Your Phone, Computer or Email* page notification, as illustrated in Figure 32. Review the available options and determine which option(s) you will use for MFA. Note that a CMS Enterprise Portal can register multiple MFA options (i.e., phone, laptop and text messaging). If necessary, download and install any software or applications necessary to that MFA option. When complete, select an option from the [Credential Type] drop-down menu.

<u>Note</u>: Regardless of the mechanism you choose, when using MFA, you will have a limited time to retrieve and enter the MFA security code. If you are unable to enter the MFA security code within that limited time, then the code will expire and you will need to request a new security code.

l		Welcome 🗢 TESTACCOUNT WIL	🕑 Help	C Lo
My Profile				
Manage Profile	Register Multi-Factor Device			
View Profile	Adding a Security Code to your login, also known as Multi-Fac login more secure by providing an extra layer of protection to to learn more about MFA and or go ahead and register your de	your user name and password. Click here		
Change Profile	Select the MFA device type that you want to			
Change Password				
Change Security Questions	Choose MFA Device	~		
Register MFA	Tablet/PC/Laptop Text Message (SMS)			
Remove MFA	Interactive Voice Response (IVR) E-mail			

#### Figure 32: Select Credential Type

 (a) /Tablet/PC/Laptop. If selecting [Phone/Tablet/PC/Laptop] as [MFA Device Type], enter the alphanumeric code that displays in the Symantec VIP Access Credential ID field, illustrated in Figure 33, into the Credential ID field, as illustrated in Figure 34. Enter a brief description in the field labeled [MFA Device Description] (i.e., "work laptop").

Figure 33: Symantec Credential ID



### Figure 34: Select Phone/Tablet/PC/Laptop as MFA Device Type

	Welcome 🔻 TES	
My Profile		
lanage Profile	Register Multi-Factor Device	
View Profile	Adding a Security Code to your login, also known as Multi-Factor Authentication (MFA), can make your login more secure by providing an extra layer of protection to your user name and password. Click here to learn more about MFA and or go ahead and register your device.	
Change Profile	to team more about with and of go anead and register your device.	
Change Password	You can associate the Security Code to your profile by registering your Phone, Computer or E-mail. Tab through the links below to find out more information about the options.	
Change Security Questions	Phone/Tablet/PC/Laptop	
Register MFA	To use the Validation and ID Protection (VIP) access software on your phone, you must download the VIP Access software to your phone, if you do not already have it. Select the following link https://m.vip.symantec.com/home.	
Remove MFA	To use VIP access software on your computer, you must download the VIP Access software, if you do not already have it. Select the following link https://idprotect.vip.symantec.com/desktop/download.	
	Text Message (SMS)	
	Interactive Voice Response (IVR)	
	E-mail	
	Select the MFA device type that you want to use to login	
	Tablet/PC/Laptop	
	Enter the alphanumeric code that displays under the label Credential ID on your device.	
	Enter Credential ID	
	Enter MFA Device Description	
	Submit	

(b) Email – One Time Password (OTP). If selecting [Email – One Time Password (OTP)] as [Credential Type], the email associated with your CMS Enterprise Portal account should be entered in the field labeled [Email Address] to obtain the one time use security code. Enter [Email] as the Credential Option, as illustrated in Figure 35.

# Figure 35: Select Email as Credential Option

rprise Portal		Welcome 👻 TESTACCOUNT WIL
Mar Droft		
My Profile		
Manage Profile	Register Multi-Factor Device	
View Profile	Adding a Security Code to your login, also known as Multi-Factor Authentication (MF login more secure by providing an extra layer of protection to your user name and pa to learn more about MFA and or go ahead and register your device.	
Change Profile	to team more about MrA and or go anead and register your device.	
Change Password	You can associate the Security Code to your profile by registering your Phone, Computer or E-n links below to find out more information about the options.	nail. Tab through the
Change Security Questions	Phone/Tablet/PC/Laptop	~
Register MFA	Text Message (SMS)	~
Remove MFA		
	Interactive Voice Response (IVR)	*
	E-mail	~
	Please note that you are only allowed two attempts to register your MFA device. If you are undevice within two attempts please log out, then log back in to try again.	able to register your
	Select the MFA device type that you want to use to login	
	E-mail	*
	The E-mail address on your profile will automatically be used for the E-mail option. Your e-mai changed at the time of MFA registration. To change your E-mail, please select 'Change E-Mail Ad 'Change My Profile' menu.	
	email_address@email.com	
	Enter MFA Device Description	
	Submit Cancel	

(c) Text Message – Short Message Service (SMS). If selecting [Text Message – Short Message Service (SMS)] as [Credential Type], enter the phone number that will be used to obtain the security code as [Phone Number] and [Text] as the Credential Option, as illustrated in Figure 36.

#### Figure 36: Select Text as Credential Option

My Profile	
Manage Profile	Register Multi-Factor Device
View Profile	Adding a Security Code to your login, also known as Multi-Factor Authentication (MFA), can make you login more secure by providing an extra layer of protection to your user name and password. Click he to learn more about MFA and or go ahead and register your device.
Change Profile	
Change Password	You can associate the Security Code to your profile by registering your Phone, Computer or E-mail. Tab through th links below to find out more information about the options.
Change Security Questions	Phone/Tablet/PC/Laptop
Register MFA	Text Message (SMS)
Remove MFA	The SMS option will send your Security Code directly to your mobile device via text message. This option require you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages Carrier service charges may apply for this option.
	Interactive Voice Response (IVR)
	E-mail
	Select the MFA device type that you want to use to login
	Text Message (SMS)
	Enter the Phone number that will be used to obtain the Security Code.
	Enter Phone Number

(d) Voice Message – Interactive Voice Response (IVR). If selecting [Voice Message – Interactive Voice Response (IVR)] as [Credential Type], enter the phone number that will be used to obtain the security code as [Phone Number] and [IVR] as the Credential Option, as illustrated in Figure 37.

#### Figure 37: Select IVR as Credential Option

tal	We	lcome 🔻 TESTACCC
My Profile		
Manage Profile	Register Multi-Factor Device	
View Profile	Adding a Security Code to your login, also known as Multi-Factor Authentication (MFA), ca login more secure by providing an extra layer of protection to your user name and passwo to learn more about MFA and or go ahead and register your device.	
Change Profile Change Password	You can associate the Security Code to your profile by registering your Phone, Computer or E-mail. The links below to find out more information about the options.	ab through the
Change Security Questions	Phone/Tablet/PC/Laptop	~
Register MFA	Text Message (SMS)	~
	Interactive Voice Response (IVR) The IVR option will communicate your Security Code through a voice message that will be sent dire phone. This option requires you to provide a valid ten (10) digits U.S. phone number and (optional) will be used during login to obtain the Security Code. The extension may begin with any one of the asterisk '*'; period '!; comma '!; pound '#', followed by numeric 0 to 9. For example: 4885554444, 1	extension that following:
	E-mail	~
	Select the MFA device type that you want to use to login	
	Interactive Voice Response (IVR)	~
	Enter the Phone number that will be used to obtain the Security Code.	
-	Enter Phone Number	
	Enter MFA Device Description	
	Submit Cancel	

Select [Submit] to continue.

7. Your registration for Multi-Factor Authentication is now complete. After [Submitting] your device type(s), you will receive an on-screen confirmation message, as illustrated in Figure 38.

<u>Note</u>: You will receive an email notification for successfully registering the MFA credential type.

#### Figure 38: Register MFA Device- Successful Confirmation Screen

Confirmation ×

# *4.3.4.2. Utilizing a Security Code When the User Does Not Have Access to Their Registered MFA Device*

If a User has registered a MFA Device but does not have access to that device, the User may utilize a self-service option to obtain a Security Code.

1. Follow the login steps outlined in <u>Section 4.3.6</u>. When the user reaches Step 4, select [Trouble Accessing Security Code?], as illustrated in Figure 39.

Figure 39: Unable to Access Security Code Begin Navigation

CMS.gov Enterprise Portal	🟥 Find Your Application 🕜 Help 🚯 About 🛛 E-Mail Alerts
	0
CMS.gov Enterprise Porto	al
VAL2016	
Password	
Choose MFA Device	
Irouble Accessing Sec	curity Code?
✓ Agree to our <u>Terms &amp; Conditions</u>	
Login	
Forgot your <u>User ID</u> or your <u>Password</u> ?	
https://portalval-beta.cms.cmsval/vps/portal/unauthportal/selfservice/unablesecuritycode/	
undes///wuraixa.neterruizruizkai/abs/hourai/neurai/seusetx/se/mianesernit/(code)	ŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢŢ

2. The *Unable to Access Security Code* self-service process begins, as illustrated in Figure 40.

#### Figure 40: Unable to Access Security Code User ID Entry

CMS.gov Enterprise Portal	Find Your Application	Help	i About	└── E-Mail Alerts
Unable to Access Security Code				
Please enter the following information to receive your one time security code for your account.				
All fields are required unless marked optional.				
Enter User ID				
Next Cancel				

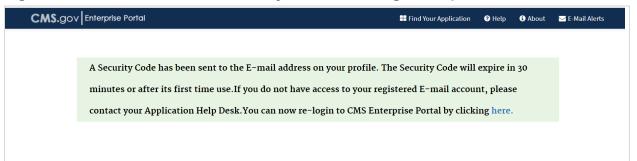
3. Enter the CMS Enterprise Portal User ID and select [Next]. The **Unable to Access Security Code** self-service process continues, as illustrated in Figure 41.

Figure 41: Unable to Access Security Code Challenge Questions

	Portal			Find Your Application	? Help	i About	└── E-Mail Alerts	^
Unable	to Access	Security Code						
Please enter the		receive your one time security co	de for your account.					
	quired unless marked '(	ptional'. mber that is not your own?						
	arve s telephone ne							
What is the n	ame of your favorit	e pet?						
What is the fi	irst name of your ol	lest niece?						
	Submit	Cancel						*

4. The User validates his/her identity by completing the challenge questions, using the answers created when the account was created. Select [Submit] to continue. The Unable to Access Security Code self-service process is completed, as illustrated in Figure 42. The CMS Enterprise Portal will send a Security Code to the User's email address on record.

#### Figure 42: Unable to Access Security Code Challenge Completion



5. After clicking [here] in Figure 42, you will be taken back to the login screen. After you have entered your User ID and Password, [click] on the Choose MFA Device drop down and [select] One Time Security code as the Device Type. Enter the security code and [click] Login, as illustrated in Figure 43.

Figure 43: Selecting One Time Security Code Option as MFA Device

CMS.gov Enterprise Portal	
testtest178	
Password	
One Time Security Code	
Enter one time security code	>
Trouble Accessing Security Code?	
Agree to our <u>Terms &amp; Conditions</u>	
Login	
Forgot your <u>User ID</u> or your <u>Password</u> ?	

# 4.3.4.3. Removing a Registered MFA Device

To remove a registered MFA phone or computer, please follow each step below.

1. Navigate to <u>https://portal.cms.gov/</u>. The *CMS Enterprise Portal* page is displayed, as illustrated in Figure 44.

#### Figure 44: CMS Enterprise Portal Screen

CMS.gov Enterprise Portal	🗮 Find Your Application 🛛 Help 🕕 About 🔤 E-mail Alerts
	CMS.gov Enterprise Portal
	DEV_TEST20
1 Am	
	Text Message (SMS)
11-14	MFA Code Sent 409964
	The Security code for the Text Message (SMS) will expire in 10 minutes,
	Trouble Accessing Security Code?
	Agree to our <u>Terms &amp; Consitions</u> Login
	Forgot your User ID or your Password?

- 2. Enter your CMS Enterprise Portal User ID, password. Then select the MFA device type, enter security code. Select the [Agree to our terms and conditions] box, and [Login].
- Registered HDT Users are required to input their Multi-Factor Authentication (MFA) credentials, selecting an MFA Device that has already been associated with the CMS Enterprise Portal User ID, and then entering the appropriate Security Code from that device. Select the [MFA Device Type] you wish to use from the drop-down menu and then enter the Security Code (VIP Token) you obtained, then select [Log In].
- 4. Select your username and then select [My Profile] from the dropdown menu to go to your profile, as illustrated in Figure 45.

# Figure 45: Select My Profile

S.gov My Enterprise Portal		Welcome TESTACCOUNT ABEL - 🕜 Help 🗇 L
		My Access
	/	My Profile
My Profile		
Manage Profile	View My Profile	Change My Profile
View Profile	First Name: TESTACCOUNT	
Change Profile	Last Name:	
Change Password	Middle Name:	
Change Security Questions	Date of Birth:	
Register MFA	E-mail Address:	
Remove MFA	Phone Number:	
	Home Address Line 1:	
	Home Address Line 2:	
	City: Baltimore	
	State: MD	
	Zip Code: 21244	
	Country: USA	

5. Select [Remove MFA] from the left navigation links to begin the process of removing an MFA device from your account, as illustrated in Figure 46.

Select the radio button next to the device you wish to remove. Enter the security code sent to your device and select [Next} to continue.

<u>Note</u>: The security code will be sent to the device that is registered. The security code is time sensitive and must be entered in a timely manner in order to complete the requested action.

# Figure 46: Remove Your Phone or Computer

My Profile				
Manage Profile	<b>Remove Multi-Factor</b>	Device		
View Profile	Credential ID/Phone #/E-mail	MFA Device Type	MFA Device Description	Remove Selected
Change Profile		Text Message (SMS)	Swati's Mobile	0
Change Password		Text Message (SMS)	Swati's Mobile	۲
Change Security Questions Register MFA Remove MFA	Select the "Send Security Code" b already registered with this accound below. Keep in mind that the Security the code promptly Send Code	nt. Once it is received o	n your phone or e-mail, ente	r the code in the text
	Security Code 443795			
		Text Message- Short Me	ssage Service (SMS) will expi	ire in 10 minutes.

6. The removal of your registered MFA device is now complete, as illustrated in Figure 47. Select [OK] to be directed to your *Profile* page.

<u>Note</u>: You will receive an email notification for successfully removing a registered MFA device from your account.

Confirmation Changes to your profile have been success	sfully submitted.			×
My Drofilo				
My Profile				
My Profile Manage Profile	Remove Multi-Factor	Device		
	Remove Multi-Factor Credential ID/Phone #/E- mail	Device MFA Device Type	MFA Device Description	Remove Selected
Manage Profile	Credential ID/Phone #/E-			Remove Selected
View Profile	Credential ID/Phone #/E- mail	MFA Device Type Tablet/PC/Laptop Interactive Voice Response	Description	
Manage Profile View Profile Change Profile	Credential ID/Phone #/E- mail	MFA Device Type Tablet/PC/Laptop	<b>Description</b> VIP	

Figure 47: Removal of Registered MFA Device Complete

# 4.3.5. Remote Identity Proofing (RIDP)

Remote Identify Proofing (RIDP) is the process of validating sufficient information about you (e.g., credit history, personal demographic information, and other indicators) to uniquely identify you. RIDP is a required service for new HETS Desktop (HDT) Users – existing HDT Users will not be required to complete the RIDP process. CMS uses Experian to remotely perform identity proofing.

The RIDP process for HDT is outlined in <u>Section 4.3.1</u>, steps 9-12. If Experian cannot identity proof you online, you will be asked to contact either the Experian Help Desk or the MCARE Help Desk, depending on the reason you failed RIDP.

The CMS Enterprise Portal will provide you with a reference number to track your case if you cannot complete identity proofing. The Experian Help Desk cannot assist you if you do not have the reference number. The Experian Help Desk can be contacted at 1-866-578-5409. The Experian Help Desk is open Monday through Friday from 8:30 AM to 10:00 PM, Saturday from 10:00 AM to 8:00 PM, and Sunday from 11:00 AM to 8:00 PM, Eastern Standard Time (EST).

For additional information, please see the Experian Consumer Assistance site: <u>Experian</u> <u>Customer Assistance</u>.

If you are asked to contact the MCARE Help Desk, you will be given a response code to help the MCARE Help Desk perform the manual identity proofing process with you. Please contact MCARE via the information provided in <u>Section 6.5</u> of this guide.

# 4.3.6. Login to the HDT Application

Follow these steps to login to the HDT application:

 Enter the CMS Applications Portal URL in a web browser: <u>https://cmshdt.cms.gov/HDT/</u>. Please do not bookmark this or any other page in your internet browser. CMS discourages Users from utilizing browser bookmarks with the HDT application. The *CMS Enterprise Portal Screen* will display as illustrated in Figure 48.

CMS.gov Enterprise Portal		Find Your Application	Help	<li>About</li>	🔀 E-mail Alerts
	CMS.gov Enterprise Port	tal	C	51	1
	UserID				
	Password	- 10			
	Agree to our <u>Terms &amp; Conditions</u>				
	Forgot your <u>User ID</u> or your <u>Password</u> ?				
	New User Registration				24
	and a second				
	About				

#### Figure 48: CMS Enterprise Portal Screen

2. Enter your CMS Enterprise Portal User ID in the User ID field.

Once you enter your CMS Enterprise Portal User ID in the **User ID** field, the *CMS Enterprise Portal Login Screen with Multi-Factor Authentication-HDT Access* will display as illustrated in Figure 49 that allows authorized Users to access the HDT application.

# Figure 49: CMS Enterprise Portal Login Screen with Multi-Factor Authentication – Access to HDT

CMS.gov Enterprise Portal	# First	d Your Application	🛛 Help 🚯 Abou	t 🔤 E-mail Alerts
	CMS.gov Enterprise Portal			0V
	DEV_TEST20			
1 Am				
	Text Message (SMS)	•		
1 American Ant	MFA Code Sent 409964			
	The Security code for the Text Message (SMS) will expire in 10 minutes.	n	1	100
	Trouble Accessing Security Co	odel		
	Login			
	Forgot your <u>User ID</u> or your <u>Password</u> ?			

- 3. Enter your CMS Enterprise Portal password in the **Password** field.
- 4. Registered HDT Users are required to input their Multi-Factor Authentication (MFA) credentials, selecting an MFA Device that has already been associated with the CMS Enterprise Portal User ID, and then entering the appropriate Security Code from that device. Select the [MFA Device Type] you wish to use from the drop-down menu and then enter the Security Code (VIP Token) you obtained, then check the [I Agree to our Terms and Conditions] if you agree, then [Log In].

#### Notes:

- If you need to register a MFA Device, select the [Register MFA Device] link and complete the process described in <u>Section 4.3.4.1.</u>
- If you have registered a MFA Device but are temporarily unable to access that device, you may utilize the [Unable to Access Security Code] link. See Section <u>4.3.4.2</u> for complete details on using this feature.
- If you enter your CMS Enterprise Portal password incorrectly three times, the system will lock your account. While your account is locked, you cannot access any other features. You must contact the MCARE Help Desk to reset your CMS Enterprise Portal password as described in <u>Section 6.5</u>.
- When an Administrator resets your CMS Enterprise Portal password, you will be sent an email with a temporary one-time password. You must then login to the CMS Enterprise Portal and change the password to one of your choice, following the CMS & HDT Password Policy. Please note that

HDT requires that CMS Enterprise Portal passwords contain only alphanumeric characters. Refer to <u>Section 4.3.3.3</u> of this document for instructions on changing your password.

5. The CMS Enterprise Portal will verify your password and MFA security code. If you are an authorized HDT user, the *HETS Desktop Home Screen (HDT-1000)* will display as illustrated in Figure 50.

Figure 50: HETS Desktop Home Screen (HDT-1000)

HETS Desktop	HETS Desktop Home	User 10: User Name: Environment:
Home NPI Nanagement * CMS HETSING Website Logout	HDT-1000 XFT Measurement	
	Centers for Medicare & Medicald Services, 7500 Security Boulevard, Baltimore, MD 21244	

# 4.4. Application Organization & Navigation

Specific functionality and screen captures are described in <u>Section 5.1</u> of this document.

# 4.5. Exiting the Application

Select the [Logout] link in the left navigation menu of any screen in the HDT Application to logout from the HDT application. You will be logged out of the HDT application and redirected to the *CMS Enterprise Portal Web Access Management (Logout) Screen* as illustrated by Figure 51.

CMS.gov Enterprise Portal	■ Find Your Application	? Help	<ol> <li>About</li> </ol>	🖂 E-mail Alerts
	CMS.gov Enterprise Portal	(	21	1
	UserID Password			
	Agree to our <u>Terms &amp; Conditions</u>			1
	Forgot your <u>User ID</u> or your <u>Password</u> ?	N		1
	New User Registration			
	About			

# Figure 51: CMS Enterprise Portal Web Access Management (Logout) Screen

If you enter your CMS Enterprise Portal User ID in the **User ID** field you will be redirected to the CMS Enterprise Portal Login Screen with Multi-Factor Authentication – Access to HDT screen (Figure 49).

# **5. USING THE APPLICATION**

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

# 5.1. Application Layout

The application layout in the Site Map, as illustrated in Figure 52, is outlined as follows:

The links to navigate through the HDT application are:

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

The links external to the HDT application are:

• CMS HETSHelp Website

#### Figure 52: HDT Application Site Map

HETS Desktop	HETS Desktop Home	Uner ID: User Name: Environment:
Home KPI Hanagament Crist HTSHebe Website Lagout NPI Batch Management PI Batch Management NPI Batch	HDT-1000 X013.Manazement	
	Centers for Medicare & Medicard Services, 7500 Security Boolevard, Baltimone, ND 21244	

When you log into the HDT application, the *HETS Desktop Home Screen (HDT-1000)* will display as illustrated in Figure 53.

#### Figure 53: HETS Desktop Home Screen (HDT-1000)

HETS Desktop	HDT-1000 MTMinagement	Uner OL Uner None Ervensteiner
	Centers for Medican & Nedicard Services, 7500 Security Boulevard, Baltonow, ND 21344	

You are able to access the functionality of the HDT application by selecting the hyperlinks from the left-hand navigation bar. Users may also select the hyperlinks in the dynamic content area in the middle of the screen.

The navigation hyperlinks are:

- Home The HDT User Interface home page.
- NPI Management Allows Submitters to add, terminate and/or query NPI numbers one at a time. This link is available to Clearinghouse and Direct Provider Submitters.
- NPI Batch Management Provides a link to the Enterprise File Transfer (EFT) system. This link is available only to Clearinghouse Submitters.
- CMS HETSHelp Website Provides links to the CMS HETSHelp Website.
- Logout Closes the active HDT application session and redirects the User to the *CMS Enterprise Portal Web Access Management (Logout) Screen* as illustrated in Figure 51.

# 5.2. NPI Management (HDT-1001)

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

To access the NPI Management feature, select the [NPI Management] link in the lefthand navigation menu. The *HDT NPI Management Screen (HDT-1001)* will display as illustrated in Figure 54.

dangeneet ' ada generg bin generge in the first of the f	<b>HETS</b> Desk	COP DOLTAGO 1) NP Managament	User ID: User Kane: Ervironment:
Submitter IO         NPI         Action Regenerated         O         Action Regenerated         O         Medicare Provider Status         O         NP/Submitter Relationship Status         O         Tansaction Flag           No data available in table	ome PI Management 45 HETSHelp ebsite gout	NPr.	
No define available in table		Story 25 • jennins	Search:
Showing 0 to 0 of 0 antrives		Submitter ID 🔺 NPI 🗘 Action Requested 🗘 Action Result 🗘 Medicare Provider Status 🗘 HETS Provider Status 🗘 NPI/Submitter Relationship Status	C Transaction Flag C
		No data available in table	
Centers for Hedicare & Hedicaid Services, 7500 Security Baulewick, Baltimore, HD 21244		Showing 0 to 0 x10 entries	
Centers for Hedicare & Hedicaid Services, 7500 Security Baulewick, Baltimore, HD 21244			
Centers for Hedicare & Hedicaid Services, 7500 Security Baulewick, Baltimore, HD 21244			
Centery for Hedicare & Hedicaid Services, 7500 Security Baulewick, Baltimore, HD 21244			
Centers for Hedicare & Hedicaid Services, 7500 Security Baulewid, Baltimore, HD 21244			
Centers for Hedicare & Hedicaré Services, 7500 Security Baulewird, Baltimore, HD 21244			
		Caster for Madrine & Madrid Gaurine - 1909 Savethe Bodawell Baltimore 107 1934	
		evenes in reasons a reason of read of Add about 1904 the Internet in Add about 1904 the Addition of Add about 1	

# Figure 54: HDT NPI Management Screen (HDT-1001)

The user selects the appropriate HETS 270/271 **Submitter ID** from the drop-down menu (depending on the related organization, there may only be one value present), enters an NPI value in the **NPI** field (HDT only accepts numeric values in this field), and the select [Add], [Query], [Terminate] or [Cancel] to proceed with the requested action.

Results for requested actions are displayed in an NPI Results table as illustrated in Figure 55.

HETS Desktop	0		(HDT-1891) NPI Management				Ner ID: Name: 
Home NPT Nanagement CMS HETSHelp Website Logout			Submitter ID: PTFVAL01  NPI:	Add Que	ry Terminate Cancel		
	Show 25 • entries					Sear	ch:
	Submitter ID 🔺						♦ Transaction Flag ♦
	PTF\/AL01	1003084492 TERMINATE	AT: RELATIONSHIP HAS ALREADY BEEN TERMINATED		ACTIVE	TERMINATED	NO
	PTF\AL01	1003084492 QUERY 1003084492 ADD	ADDED	VALID	ACTIVE	ACTIVE	YES
	Showing 1 to 3 of 3 entries	5					
			Centers for Medicare & Medicaid Services. 7300	Servity Builevard Baltimore MD 21244			
			central of montal e of Hebitalio Services, 700	security addresses, saturate, no 21244			

# Figure 55: HDT NPI Management Screen (HDT-1001) - Results

The following information is provided for each action selected:

- Submitter ID the 8-character Submitter ID selected by the User.
- NPI NPI entered by the User.
- Action Requested the action button selected by the User. Values include:
  - Query this action is selected by the User to determine the status of the relationship between the Submitter ID and the NPI entered.
  - Add this action is selected by the User to create a relationship between a Submitter ID and an NPI for the purpose of submitting 270 request transactions via the HETS 270/271 application.
  - Terminate this action is selected by the User when a Submitter no longer has a business relationship with an NPI.
- Action Result the result returned by HDT based on the action selected by the User. Values include:
  - Queried the query request has been processed by the HDT application and the query results are displayed in the NPI results table.
  - Added the NPI/Submitter relationship has been added to the HDT application.
  - AE: Relationship Already Exists the NPI/Submitter relationship already exists and cannot be added.
  - SP: Relationship is Suspended the NPI/Submitter relationship is currently suspended and cannot be added.
  - IM: Invalid Medicare Provider Status the Medicare Provider Status is invalid and cannot be added.

- Terminated the NPI/Submitter relationship has been terminated in the HDT application.
- AT: Already Terminated the NPI/Submitter relationship is already terminated and cannot be terminated.
- NE: Relationship Does Not Exist 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.
- Medicare Provider Status this status indicates whether or not 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. Values include:
  - 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. Values include:
  - 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.
- Transaction Flag this status flag indicates whether or not transactions with the HETS 270/271 application are permitted. Values include:
  - Yes Indicates that transactions with the HETS 270/271 application are permitted. This value is returned when all of these 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".

<u>Note</u>: The table will display the results in the order in which the NPIs are entered into the NPI text box, with the most recent action listed first. The HDT application defaults to display up to 25 rows in the NPI Results table. The user can change this value in the 'Show \_\_\_\_ Entries' dropdown to modify the results parameters.

# 5.2.1. Query

#### 5.2.1.1. Action

The Query action allows Submitters to verify NPI numbers prior to submitting a 270 request transaction to the HETS 270/271 application. Responses are returned to the screen in a matter of seconds.

To perform a query action, follow these steps on the *HDT User Interface NPI Management Screen* as illustrated in Figure 56:

Figure 56: HDT NPI Management Screen (HDT-1001) – Query

HETS	Deskto	D	(JCT-1011) WP Mangement		User 10: User Name: Environment:
Home NPI Management CMS HETSHelp Website Logout			Submitter ID: CTFVALC2	Add Query Terminate Cancel	
		Show 25  entries Submitter ID  NPI Action Requested	Action Result     Medicare Provider Status	HETS Provider Status     NPI/Submitter Relationship S	Search: Search Status O Transaction Flag O
		Submitter ID A NPI C Action Requested	Action Result     Medicare Provider Status     No data avail		tatus 0 Transaction Hag 0
		Showing 0 to 0 of 0 entries			
			Centers for Medicare & Medicaid Services, 7300 Security Boulevard, Ba	altimore, MD 21244	

- 1. Select a Submitter ID from the drop-down list 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 [Query].

<u>Note</u>: The HDT application will clear the **NPI** field when you select an NPI Management action. The Submitter ID field will not be cleared. If you wish to perform actions for a different Submitter ID associated with your

Submitter Profile, you must select that Submitter ID from the Submitter ID drop-down list.

#### 5.2.1.2. Result

Figure 57 displays the NPI Results table for the query action.

Figure 57: HDT NPI Management Screen (HDT-1001) – Query Results

HETS Desktop	) (607-5041) MP Management	User10: UserName: Environment:
Home NPI Management CMS HETSHelp Websile Logout	Submitter f0: CTFVALC2 • NPE Add Query Terminate Cancel	
	Show 25 V entries	Search:
	Submitter ID 🔺 NPI 🗘 Action Requested 🗘 Action Result 🗘 Medicare Provider Status 🗘 HET'S Provider Status 🗘 NPI/Submitter Relationship Status	Transaction Flag
	CTF/IALC2         10030844/2         QUERY         QUERED         VALID         ACTIVE         NOT FOUND	NO
	Showing 1 to 1 of 1 entries	
	Centers for Medicare & Medicaid Sarvices, 7500 Security Boulevard, Baltimore, MD 21244	

# 5.2.2. Add

The Add action creates a relationship between a Submitter ID and an NPI necessary for 270 request transactions to successfully process via the HETS 270/271 application. If you 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, then a 271 AAA error will be returned instead of entitlement information.

# 5.2.2.1. Action

To perform the add action; follow these steps on the *HDT User Interface NPI Management Screen* as illustrated in Figure 58:

HETS	Deskto	p	(NCF.1091) NP Mangement		UserID: UserName: Environment:
Home NPI Management CMS HETSHelp Website			Submitter ID: CTFVALC2   NPI: 1003084492		
Logout				Add Query Terminate Cancel	
		Show 25  entries			Search:
		Submitter ID * NPI   Action Requested	Action Result     Medicare Provider Status     No data avail	HETS Provider Status     NPI/Submitter Relationship  kobe in table	Status O Transaction Flag O
		Showing 0 to 0 of 0 entries			
			Centers for Medicare & Medicaid Services, 7500 Security Boulevard, B	altimore, MD 21244	

# Figure 58: HDT NPI Management Screen (HDT-1001) – Add

- 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 [Add].

<u>Note</u>: The HDT application will clear the **NPI** field when you select an NPI Management action. The Submitter ID field will not be cleared. If you wish to perform actions for a different Submitter ID associated with your Submitter Profile, you must select that Submitter ID from the Submitter ID drop-down list.

#### 5.2.2.2. Result

Figure 59 displays the NPI Results table for the Add action.

HETS	Deskto	p	(ACT1001) MPI Management		User ID: User Manne: Environment:
Home NPI Management * CMS HETSHelp Website Logout			Submitter ID: CTFVALC2  NPI:	Add Query Terminate Cancel	
		Show 25 • entries			Search:
		Submitter ID A NPI C Action Requested	Action Result     Medicare Provider Status	HET'S Provider Status     NPU'Submitter Relationshi	Status C Transaction Flag C
		CTF\ALC2 1003084492 ADD	ADDED VALID	ACTIVE ACTIVE	YES
		Showing 1 to 1 of 1 entries			
			Centers for Medicare & Medicaid Services. 7500 Security Boulevard. B	laltimore, MD 21244	

# Figure 59: HDT NPI Management Screen (HDT-1001) – Add Results

#### 5.2.3. 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, you will be unable to submit eligibility transactions via the HETS 270/271 application for the NPI.

#### 5.2.3.1. Action

To perform the terminate action; follow these steps on the *HDT NPI Management* – *Terminate Screen* as illustrated in Figure 60:

HETS Deskto	qq		(HDT-1001)	NPi Management							User ID: User Name: Environment:	
ome Pf Mangement 45 HTTSHelp 455HT 1990t				CTFVALC2 •		Add	Query	Terminate	Cancel			
	Show 25 • entries										Search	
	Submitter ID + N	PI 0 Action Requested	0 A	ction Result 0	Medicare Provider Status	٥	HET'S Pr	ovider Status	¢	NPI/Submitter Relationship Status	0	Transaction Flag 0
					No data av	alable in table						
	Showing D to 0 of 0 entities											

# Figure 60: HDT User Interface NPI Management Screen (HDT-1001) – Terminate

- 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 [Terminate].

<u>Note</u>: The HDT application will clear the **NPI** field when you select an NPI Management action. The Submitter ID field will not be cleared. If you wish to perform actions for a different Submitter ID associated with your Submitter Profile, you must select that Submitter ID from the Submitter ID drop-down list.

#### 5.2.3.2. Result

Figure 61 displays the NPI Results table for the terminate action.

ETS Desk	top	(PCT-1011) MPI Wanagement		Utwar KD; Utwar Kannar Environment;
ngamurat * Situlp		Subanter Dr. (CTP/ALC2)	Add Query Terminute Cancel	
	Show 25 * ansies			Search:
	Submitter ID + NPI 0 Action Requested	0 Action Result 0 Medicare Pro-	vider Status 0 HET's Provider Status 0	NPI/Submitter Relationship Status 0 Transaction Flag
	CTP-IALC2 1003054492 TERMINATE	AT RELATIONSHIP HAS ALREADY BEEN TERMINATED VALID	ACTIVE	TERMINITED NO
	Showing 1 to 2 of 2 writins			

# Figure 61: HDT NPI Management Screen (HDT-1001) – Terminate Results

# 5.3. NPI Batch Management

NPI Batch Management is available to Clearinghouse Submitters only. This feature allows you to query, add, and/or terminate more than one NPI number at a time.

NPI Batch Management screen will also allow users to complete the following:

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

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

To access the NPI Management feature, select the [NPI Batch Management] link in the left-hand navigation menu as illustrated by Figure 62 below. The *HDT NPI Batch Management Screen (HDT-1002)* will display as described in <u>Section 5.3.3</u>.

HETS Deskt	ор	METS Guidago Marrin HDT-1000	User D. Uve Rese Environment
Home		NPI Management	
NPI Management	NPI Management		
CMS HETSHelp Website Logout	NPI Batch Management		
Logour			
		Centers for Medicare & Medicaid Services, 7500 Security Boulevard, Baltimore, ND 21244	

# Figure 62. NPI Batch Management Menu Navigation

# 5.3.1. 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 Table 3 for the Input File Layout and a description of elements.

Data Element	Data Type	Length	Possible Values	Description
Submitter ID	Alphanumeric	8		The 8-character Submitter ID associated with the Clearinghouse.
NPI	Numeric	10		The 10-digit NPI for whom the Clearinghouse will be sending eligibility transactions to the HETS 270/271 application.
Action	Alpha	1	Q, A, or T	The action requested by the Clearinghouse to query the current 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.

Table 3: Input File Layout and	<b>Element Description</b>
--------------------------------	----------------------------

# Sample Input File

```
File Name: C123A456.IN.HDT.EFT
C123A456,111111111,Q
C123A456,222222222,Q
C123A456,3333333333,A
C123A456,444444444,A
C123A456,4444444444,A
C123A456,555555555,A
C123A456,6666666666,T
C123A456,6666666666,T
C123A456,777777777,T
```

# 5.3.2. 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 exception of the addition of the date and time stamp of when the file was processed and status responses appended to each line.

If the NPI Batch Management input file contains an NPI which is not equal to 10 characters 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 for the Output File Layout and a description of elements.

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

# Table 4: Output File Layout

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.

Data Element	Data Type	Possible Values	Description
Submitter Status	Alpha	A, S or T	The status of the Submitter in the HDT application. Values include: A: The Submitter is active and authorized to conduct HETS 270/271 transactions. S: The Submitter is suspended and not authorized to conduct HETS 270/271 transactions. Please contact MCARE for additional information. T: The Submitter has been terminated and is not authorized to conduct HETS 270/271 transactions. Please contact MCARE for additional information.
Medicare Provider Status	Alpha	V or I	The status that indicates whether or not 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.
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.

Data Element	Data Type	Possible Values	Description
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 is expired for the HETS 270/271 application.
Transaction Flag	Alpha	Y or N	The status flag that indicates whether or not 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 all of the following conditions are met:
			Submitter Status = A
			Medicare Provider Status = V
			HETS Provider Status = A
			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

```
C123A456,111111111,Q,Q,A,V,A,A,Y
C123A456,22222222,Q,Q,A,I,T,T,N
C123A456,333333333,A,A,A,V,A,A,Y
C123A456,333333333,A,AE,A,V,A,A,Y
C123A456,444444444,A,SP,A,V,S,S,N
C123A456,555555555,A,IM,A,I,NF,NF,N
C123A456,66666666666,T,T,A,V,A,T,N
C123A456,66666666666,T,AT,A,V,A,T,N
C123A456,77777777,T,NE,A,I,NF,NF,N
```

<u>Note</u>: 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.

# 5.3.3. Viewing 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 (HDT-1002)* will display as illustrated in Figure 63.

	0 🔒 https://htt.hets-test.mp.ansdoud.local(HD)/ Sunnel 📋 0.65						⊠ ☆	N 0 \$
HETS			(HOTHOD) SPIEwon	laragement				User ID: ASHLIVE User Kans: e usik ashk Environment: TEST
Home	CSWACTSTJRUHDTEFTD19H08LT1660006.at - IN-PR	1002555						
NPI Ranagement *	The required file format is Su	ubmitter/D.IN.HDT.EFT. Ple	ase browse to	select file.				
Trading Partner , Management		Filename: Choose File		Br	DWSE			
System Husitoring ' System , Administration CNS HETSIAIA		Upload Car	cel					
CHS HETSHelp Website Logout	Stow 25 wettes						Press Enter to Search	
	Input File	0	Size 0	Satus	Created Date		Output File	0
	CSNACTST IN HOT VAPO191028 T0908046 M		15876 S	CCESS	10/26/2019 09/08 46:165	CRIACTSTOP	CHOTI VIAP DHISHIZE TISHIKAK SH	
	CSNACTSTIN KOTEPTID 191125 T1152080 M		13 S	CCESS	10252019 105240380	CRIACTSTOP	CHOTEFT.0114125.1145280.5d	
	CSNACTSTIX HOTEPTICHENES TRENENT M		6100 SI	CCESS	1025201918191170			
	Stowing 1 to 3 of 3 entries							

# Figure 63: HDT-1002 NPI Batch Management Screen

# 5.3.4. Uploading a File

To upload an input file, follow these steps:

1. On the **HDT-1002 NPI Batch Management screen**, illustrated in Figure 63, select [Browse]. A pop-up will open (as illustrated by Figure 64.) and allow you to select the file from your local device.

#### Figure 64: Select Upload File for Processing

🕂 🕆 🛉 This	re / bestop		* 0	Search Desktop		P									
rganize • New folder				811	• 🔳	0							☑ ☆	± ⊪	
This PC	Name	Date modified	Туре	Size		1									
3D Objects	IRA IRA	8/28/2018 12:37 PM	File folder												User ID: A
Desktop	apache-jmeter-2.13	8/28/2018 12:38 PM	File folder												er Name:
Documents	sqldeveloper-4.0.2.15.21-x64	8/29/2018 12:13 PM	File folder			- 1	Manag	ement						Enviro	onment
Downloads	SoapUIProjects	9/18/2018 2:02 PM	File folder												
	CWR insurance stuff	9/27/2018 7:56 AM	File folder				-								
Music	get_prvdr_hstry_details_pl11688	11/20/2018 11:33	File folder												
Pictures	SoapUl_inputs	2/1/2019 12:24 PM	File folder					In case of the local division of the local d							
Videos	MEIC	2/13/2019 12:33 PM	File folder					Browse							
Windows (C:)	jMeter	3/18/2019 7:57 AM	File folder												
- Stephen.Swartz (	new benes sql	3/28/2019 9:49 AM	File folder												
Common (\\f17	Replacement Regression	6/24/2019 10:30 AM	File folder												
Programs (\\f17	UFT_Screenshots	6/26/2019 9:10 AM	File folder												
	Closed Tickets	7/9/2019 1:50 PM	File folder										Press Enter to Search		
Trash (\\f1710-fs	AWS benes	7/16/2019 12:54 PM	File folder										These criter to starter		
BESST (\\f1710-t	Timesheets	8/8/2019 3:28 PM	File folder				tatus		0	Created	I Date	¢	Output File		
v	TransmissionTool	0/5/2010 7-53 AM	File folder				-	No data	available in table						
File nan	ne		~	All Files (".")		~	-								
				Open	Cano	el									
				Open	Cano	el									ļ

- 2. Select the comma delimited, flat text file containing the multiple NPIs you wish to query, add and/or terminate. Then select [Open].
- Select [Upload]. Once the file has finished uploading, HDT will display the message "SubmitterIND.IN.HDT.EFT. YYMMDD.XXXXXXX.txt \*IN-PROCESS". The HDT-1002 NPI Batch Management screen will be updated to show the file in process as illustrated in Figure 65.

#### Figure 65: Submitted File – In Progress Verification and Output File

HETS D	esktop	(HDT-1002) IIPI Eatch Management				User ID: ASHLN User Name: e ashin Environment: TEST
ome	CSWACTST.IN. HDT.EFT.D191028.T1600036.bt - IN-PROCESS					
PI Management )	The required file format is SubmitterID.IN.HDT.EFT or SubmitterID.IN.I	DT.VAP. Please browse to select file.				
ading Partner , anagement	Filename	Choose File	owse			
ystem Monitoring						
ard and						
		Upload Cancel				
IS HETSHelp ebsite		Upload Cancel				
rstem , dministration , IS HETSHelp lebsite lebsite	Stow 25 v etties	Upload Cancel			Press Enter to Search	
S HETSHelp ebsite	Stow 25 v entres		Created Date	×	Press Enter to Search Output File	\$
IS HETSHelp ebsite			Created Date Created Date 10/28/2019 09 06 46165	* <u>CsineCTST.00TA0TA0APdres2T0</u>	Output File	\$
IS HETSHelp ebsite	Input File	♦ Size ♦ Status			Output File	

# 5.3.5. Downloading Output File

To download a results file, follow these steps:

- 1. Select the appropriate Output File that you would like to review. An *EFT File Download* pop-up window will display as illustrated in Figure 66.
- 2. Select the **HDT-1002 NPI Batch Management** page following the steps in **Section 5.3**. Recent batch files will display in the Submitter Output File list, including input file name, file size, file processing status, created date and, if applicable, a link to the batch response file in the Output File column (as illustrated in Figure 66).
- 3. Select [Save]. The file will be saved as the default file name of the HDT Batch output file. You may rename the file at your discretion once the file is saved to your computer.
- 4. Select [Cancel] if you decide not to save the results file.

#### Figure 66: EFT File Download

nagement *	The required file format	is SubmitterID.IN.HD1	EFT. Please browse to s	elect a file.	
Partner - ment - Nonitoring -		Upload Cancel			
tudion * Shelp	See 3 -			Pesa Enter ta Saard	1
	Input File	0 Sor 0 Solo	o Centedate ·	Culput File	
	CRIACISTA HET SPEDIALES THEOREM	10 \$60255	10252119 10:5212.000	CRECTORNED TO HIS THREE M	
	CONSTRUCTORY OF THE SET OF	ente success	102520918191170		
	Storing ( to 2 of 2 within				

# 5.3.6. Invalid File Name Format Error Message

If a HDT user from a clearinghouse attempts to upload a batch input file that does not meet the required naming convention specified in <u>Section 5.3.1</u>, HDT will return an error message on the **HDT-1002 NPI Batch Management** page as illustrated in **Figure 67**.

# Figure 67: Invalid File Name Format

HETS	Desktoj	0			(HD	F1002) NPI Batch Management					User ID: ASHLIN1E User Name: Environment:
Home		The required file format is S	ubmitterID	.IN.HDT.EFT. P	lease brow	vse to select a file.					
NPI Management			_				_				
Trading Partner , Management			File	name: Choose File		Bro	owse				
System Monitoring				Upload	Cancel						
System ) Administration				Opioau	Cancer						
CMS HETSHelp Website		EPOR1113 - Files not found									
Logout		Show 25 v entries								Press Enter to Search	
		Input File	*	Size	\$	Status	¢	Created Date	¢	Output File	0
						,	io data available in table				
		Showing 0 to 0 of 0 entries									

# 6. TROUBLESHOOTING & SUPPORT

# 6.1. 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 6AM – 11:59PM ET Tuesday 6AM – 11:59PM ET Wednesday 6AM – 11:59PM ET Thursday 6AM – 11:59PM ET Friday 6AM – 11:59PM ET Saturday 12AM – 11:59PM ET Sunday 12AM – 6:59PM, 9PM – 11:59PM ET

You may be able to login to the HDT application outside these days/times, but the NPI Management functionality will be disabled. If you 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 you submit a batch file that does not complete processing before the system becomes unavailable, the batch output file will include an error message that the file could not be processed. The Submitter will need to upload the file again when the HDT database is available.

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

# 6.2. Connectivity

If you experience any problems while using the HDT application, contact the MCARE Help Desk. For contact information for the MCARE Help Desk, refer to <u>Section 6.5</u>.

# 6.3. Error Messages

# 6.3.1. Access and Behavior Error Messages

HDT returns a variety of unique errors related to User access or behavior issues. Table 5 provides a complete list of these errors. Each error displays a specific recommendation on screen. Users should follow the on screen recommendations. When directed to do so, Users should take note of the error message they received and then contact the MCARE Help Desk for assistance. For contact information for the MCARE Help Desk, refer to Section 6.5.

Table 5: A	ccess and	Behavior	Error	Messages
------------	-----------	----------	-------	----------

Error Message
Message 100
Message 110
Message 120
Message 130
Message 700
Message 710
Message 720
Message 730
Message 740
Message 750
Error while processing your request. Please try again.

# 6.3.2. CMS Enterprise Portal Login

If you enter an incorrect/invalid CMS Enterprise Portal User ID, password or MFA Security Code, the *Incorrect ID, Password or Security Code Screen* will display the message as illustrated in Figure 68.

CMS.gov Enterprise Portal		H Find Your Application	🕑 Help 🚯 About 🔤 E-Mail Alerts
	CMS.gov Enterprise Portal		
	Cogin Error × Incorrect combination of User ID/Password/MFA Security code. Please try again.		
the comme	UserID		
	Password		
	Agree to our Terms & Conditions		
	Login		
	Forgot your <u>User ID</u> or your <u>Password</u> ?		
and the second s			
1	New User Registration		
1			

Figure 68: Incorrect ID, Password or Security Code Screen

Enter a valid CMS Enterprise Portal User ID in the User ID field. Select [Next].

If you have forgotten your CMS Enterprise Portal User ID or password, refer to <u>Section</u> <u>4.3.3</u> for more information. If you continue to encounter issues logging into the CMS Enterprise Portal, please refer to <u>Section 6.5</u> and contact the MCARE Help Desk.

# 6.3.3. Missing or Invalid NPI

On the *NPI Management* (HDT-1001) screen, if you do not enter an NPI number prior to clicking on an action button, or if you enter an invalid NPI format, the NPI Results table will return a response that includes the value you entered in the NPI field as well as a Medicare Provider Status of Invalid. Refer to Figure 69 for an illustration.

Figure 69: NPI Management -	- Invalid NPI Screen
-----------------------------	----------------------

IETS Deskto	D (HC7.1091) NV Margament En	User ID: User Name: invironment:	
	P (PACIENT) AC MANAGEMEN		
anagement • ETSHelp Be	Submitter (Dr. (PTF/AL01 * )		
	Add Query Terminate Cancel		

# 6.3.4. Batch File Error Messages

Table 6 identifies the error messages that will be returned in the output file when the input file cannot be processed for the indicated reasons.

#### Table 6: 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 3 requisite elements.
Line #\${lineNumber}: Action must be either A, Q, or T	A line in the batch file does not include one of the 3 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 is greater than 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	The Submitter ID within the file is:
invalid. File could not be processed	Not found,
further.	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.

# 6.4. Special Considerations

# 6.4.1. Data Size Limits

There is no limit to the NPI Batch Management input file size accepted by the HDT application; however, the EFT file transfer system has a file size limitation of 1GB.

# 6.4.2. Daily Batch File Submission

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

# 6.5. System Support Information

If problems and/or questions arise while accessing the HDT application, contact the MCARE Help Desk at 1-866-324-7315 or at <u>MCARE@cms.hhs.gov</u> Monday through Friday, from 7:00 AM to 7:00 PM ET.

<u>Note</u>: MCARE email is monitored during normal business hours. Emails are typically answered within one business day.

# 7. GLOSSARY

Term	Definition
HETS 270/271 Application	The HETS 270/271 application provides access to Medicare Beneficiary eligibility data in a real-time environment. Submitters may initiate a real-time 270 eligibility request to query coverage information from Medicare on patients for whom services are scheduled or have already been delivered. In real-time mode, the Submitter transmits a 270 request and remains connected while the application processes the transaction and return a 271 response.
HETS Desktop (HDT	The HETS Desktop (HDT) application is used by HETS 270/271 Submitters to register and maintain an up-to-date record of their business relationships with their Medicare Provider and/or Supplier customers prior to submitting HETS 270/271 transactions. In addition, Submitters are able to verify if NPI numbers are eligible for use with the HETS 270/271 application
Submitter	A Clearinghouse and/or Direct Provider who conducts eligibility transactions via the HETS 270/271 application
Submitter ID	The ID assigned by CMS that allows a Clearinghouse or a Direct Provider to conduct eligibility transactions via the HETS 270/271 application.
User	A person who requires and/or has acquired access to the HDT application.

# 8. ACRONYMS

Table 7 identifies acronyms and definitions used in this document.

Acronym	Definition
CMS	Centers for Medicare & Medicaid Services
EIDM	Enterprise Identity Management system – also known as the CMS Enterprise Portal
EFT	Enterprise File Transfer system
ET	Eastern Time
FFS	Fee For Service
HDT	HETS Desktop
HETS	HIPAA Eligibility Transaction System
MCARE	Medicare Customer Assistance Regarding Eligibility
MFA	Multi-Factor Authentication
NPI	National Provider Identifier
PHI	Protected Health Information
RIDP	Remote Identity Proofing