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

Final

Version: 1-9

Effective Date: July 2018

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.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

This user guide provides the information necessary for Clearinghouse and Direct Provider Submitters to effectively use the HIPAA Eligibility Transaction System (HETS) Desktop (HDT) application.

The Centers for Medicare and 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 Section 3 and may be accessed via this website link:

http://cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/HETSHelp/Downloads/HETS270271CompanionGuide5010.pdf

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/CMS-EIDM-User-Guide.pdf

If problems and/or questions arise while accessing the HDT application, contact the MCARE Help Desk at 1-866-324-7315 or at MCARE@cms.hhs.gov 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.

Table 2: Typographical Conventions

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.	Hyperlink
Note	Denotes important information and are represented as mixed-case, underlined text followed by a colon.	Note:

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:

- Internet Explorer 8, 9, 10, and 11
- Mozilla Firefox
- Chrome
- Safari

CMS recommends the Chrome internet browser for HDT Users.

HDT Users should follow the login process outlined in Section 4.3.6 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.

4.1.1. Internet Explorer

To ensure you are using the recommended settings for Internet Explorer, perform the following:

1. Go to the Internet Explorer [Tools] Menu.
2. Go to [Compatibility View Settings]
3. If present, remove https://hdt.cms.gov from the list of websites used with Compatibility View.
4. Next, select [Internet Options] from the Internet Explorer [Tools] Menu.
5. Select the [Settings] button under the Browsing history section on the General tab.
6. On the Temporary Internet Files tab, ensure that the [Every time I visit the webpage] button is selected under the section: [Internet Explorer stores copies of webpages, images and media for faster viewing later]

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 passwords contain alphanumeric characters only. Special characters such as '@', '–', '_' and '.' (dot/period) 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 will not be granted access to the HDT application. CMS Enterprise Portal Users that utilize HDT should also ensure that their CMS Enterprise Portal password does not contain any special characters.

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.

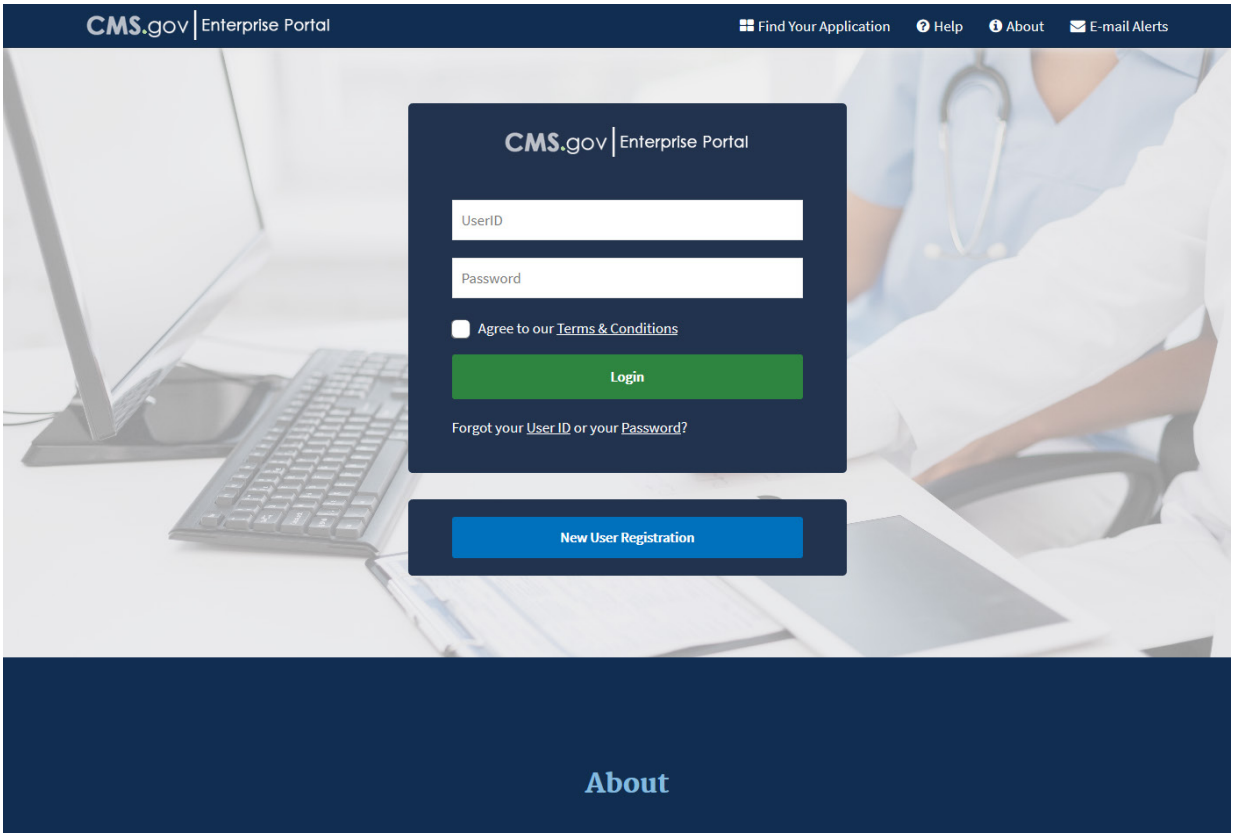
4.3.1. Requesting HDT Access for an Existing CMS Enterprise Portal Account

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

Note: 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.

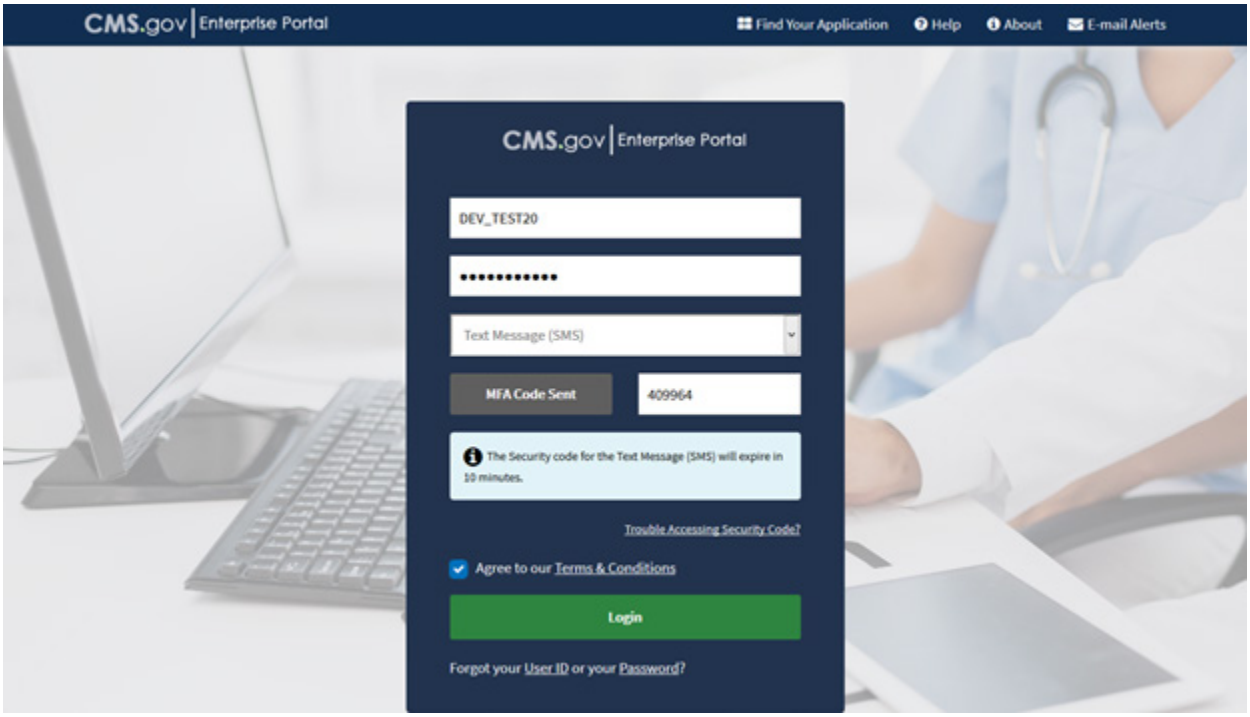
1. Navigate to https://portal.cms.gov/. The ***CMS Enterprise Portal*** page is displayed, as illustrated in Figure 1.

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

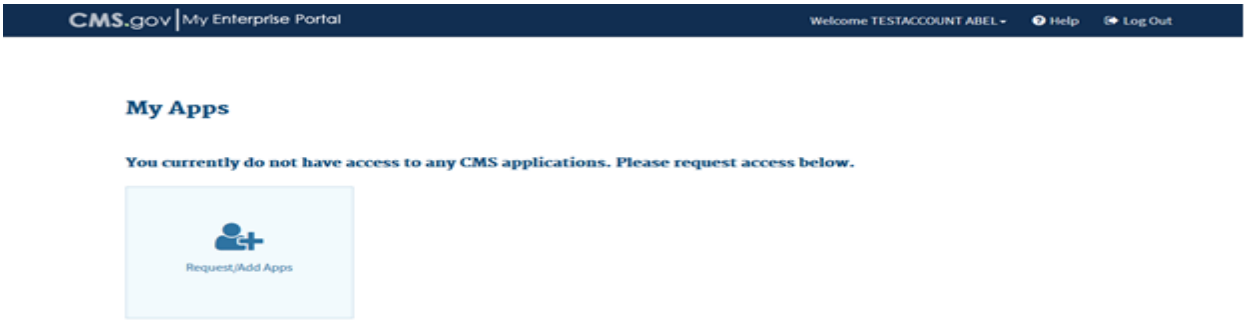


Notes:

- If you need to register a MFA Device, select the [Register MFA Device] link and complete the process described in Section 4.3.4.1.
- 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 4.3.4.2 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 Section 6.5.
- 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 Section 4.3.3.3 of this document for instructions on changing your password.

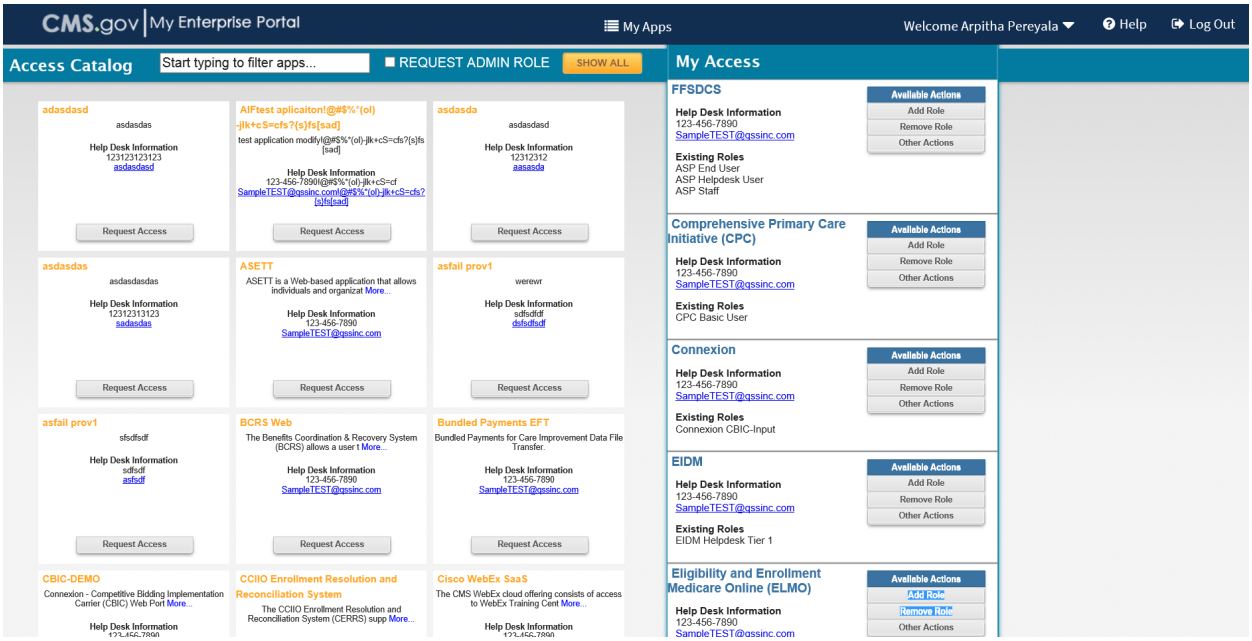
5. After logging in, the ***My Apps*** page is displayed, as illustrated in Figure 3. Select the [Request/Add Apps icon] that appears under My Apps. Alternately, you may select [down arrow icon] that appears next to your name at the top of the page to continue.

Figure 3: My Access Screen



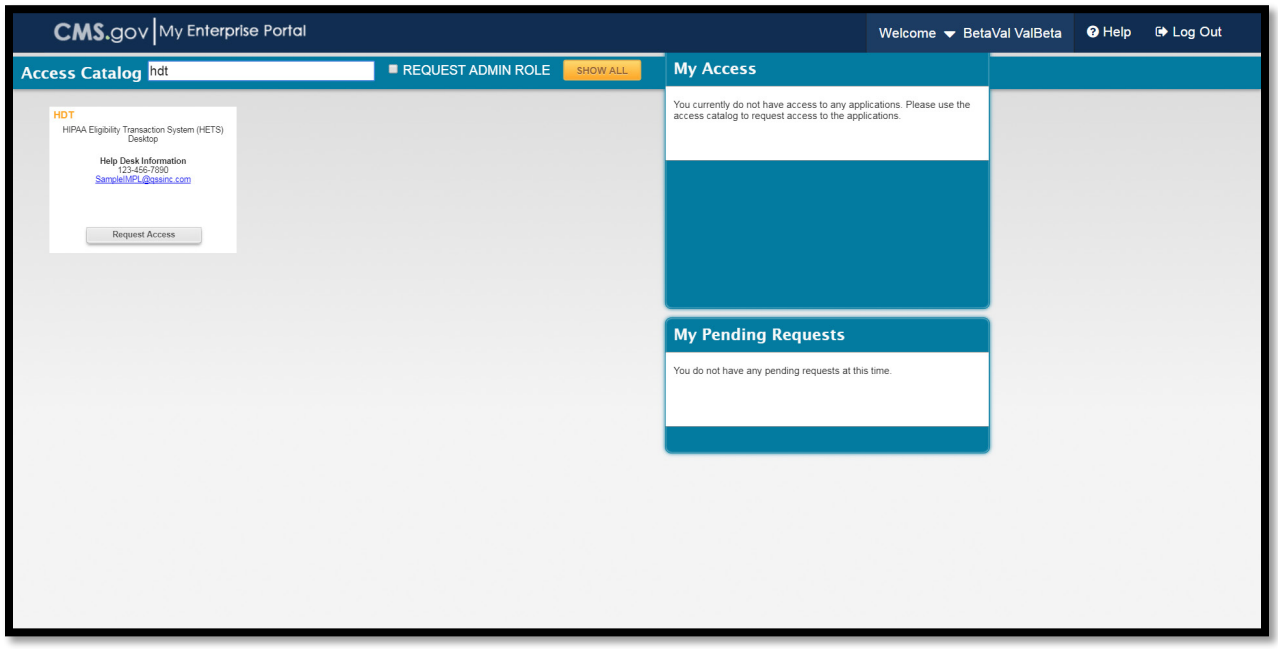
6. The [Access Catalog], [My Access] and [My Pending Requests] sections are displayed, as illustrated in Figure 4. Scroll down to locate the application you need, if it is not displayed. Alternatively, enter the first few letters of the application in the [Search] section and all of the applications beginning with those letters will be displayed. Note: 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



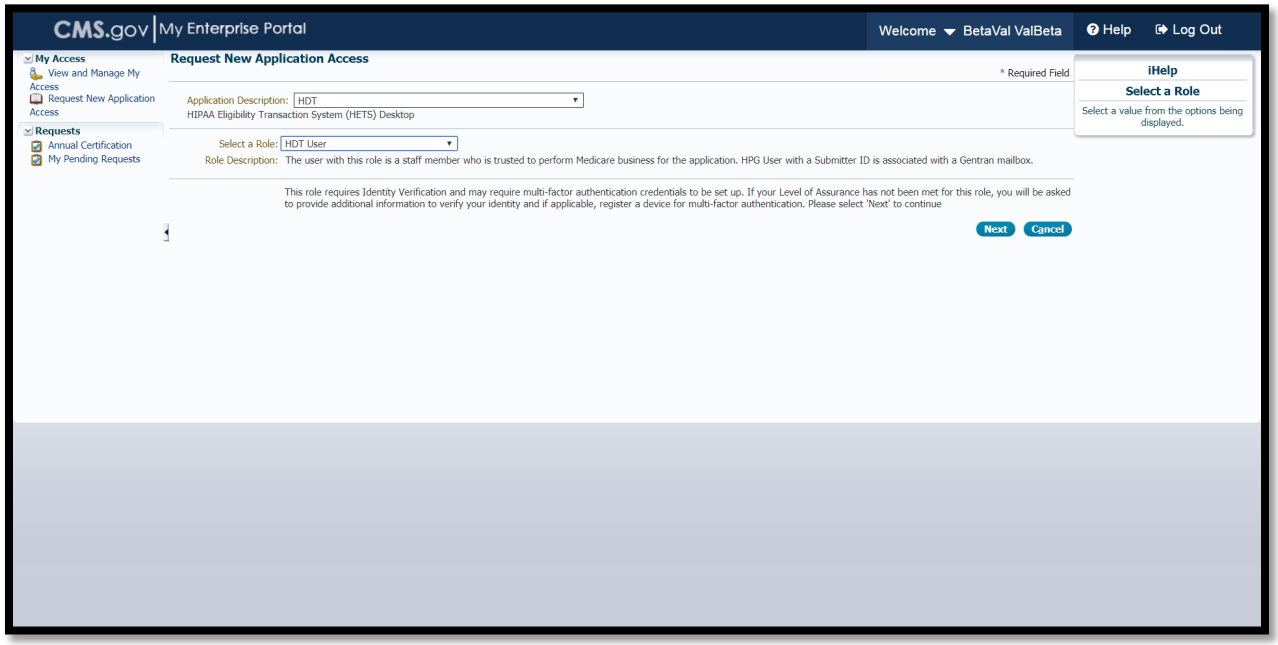
7. After entering the first few letters of the application in [Search], the applications beginning with those letters are displayed, as illustrated in Figure 5. Select [Request Access] for the HETS Desktop (HDT) role.

Figure 5: Request Access



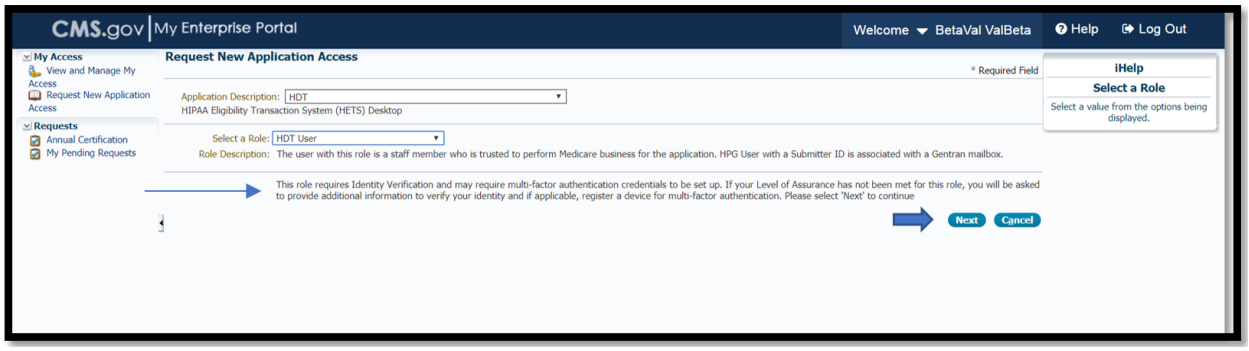
8. The Application Description and Select a role sections are displayed, as illustrated in Figure 6. Select the HDT User role from the [Select a Role] drop down menu.

Figure 6: Select a Role



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



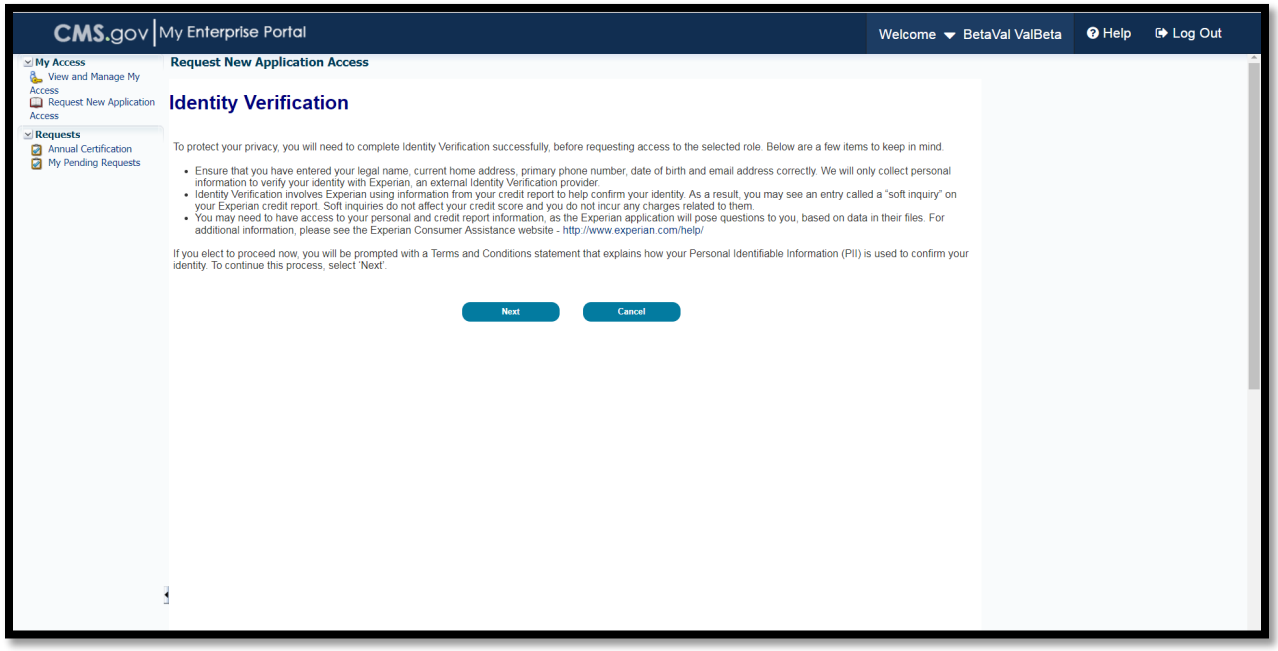
9. Depending on your CMS Enterprise Portal account, you may now be directed to the ***Identify Verification*** page, as illustrated in Figure 8. This identify verification process (Remote Identity Proofing or RIDP) is used to verify your identity and is done by asking questions based on your personal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

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

   Note: 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.

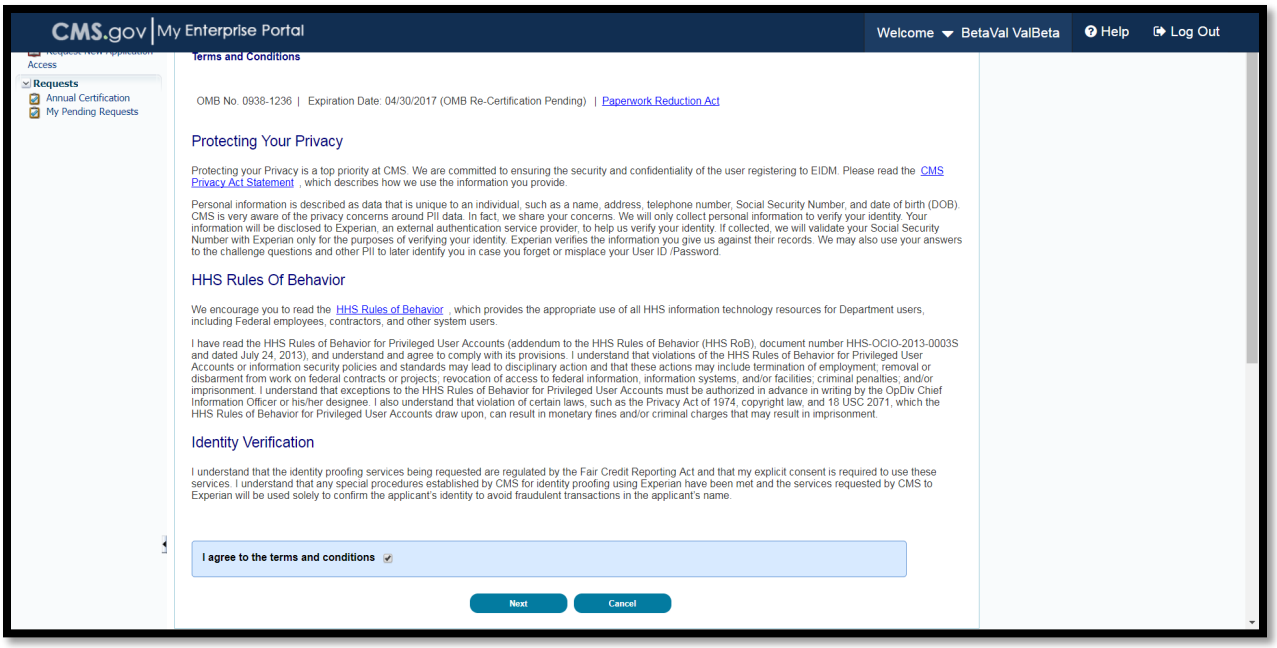
Figure 8: Identity Verification Screen



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].

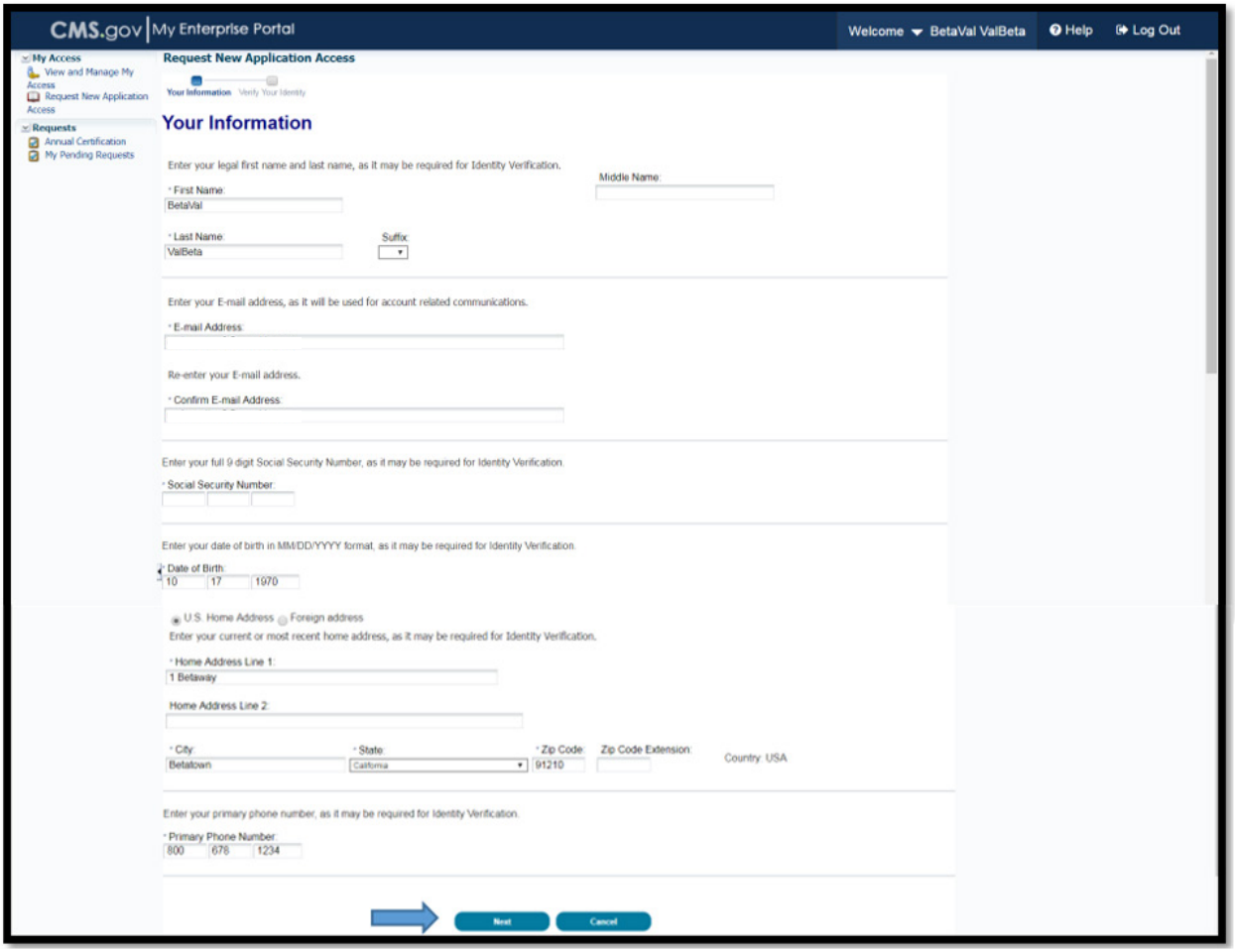
    Note: [Next] will be enabled only after checking the [I agree to the terms and conditions] checkbox.

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.

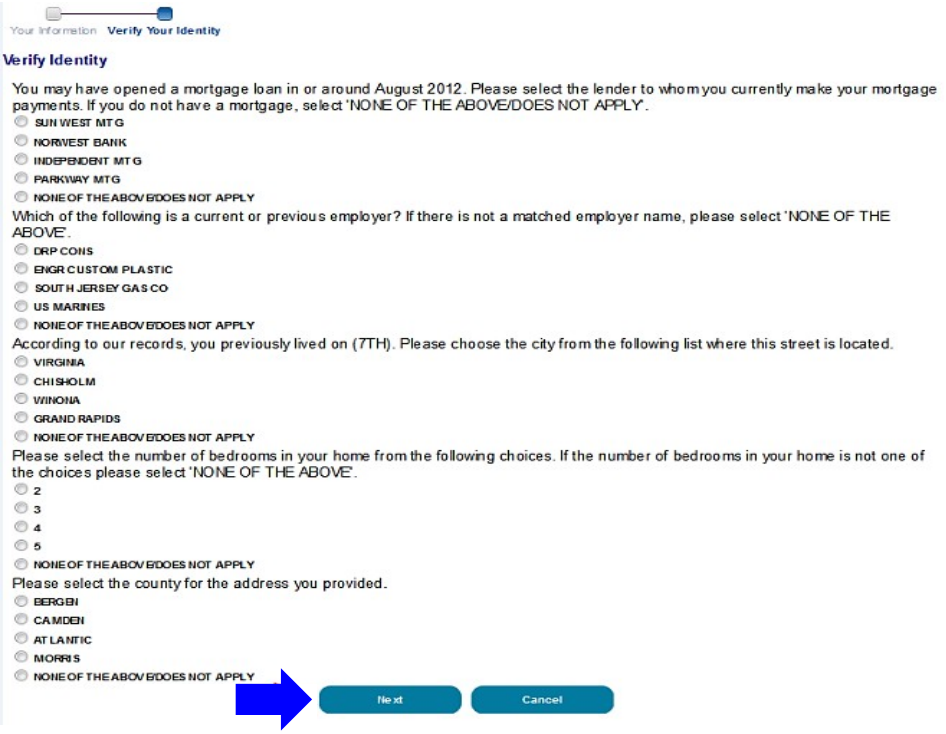
Figure 10: Your Information Screen



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.

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

Figure 11: Verify Identity

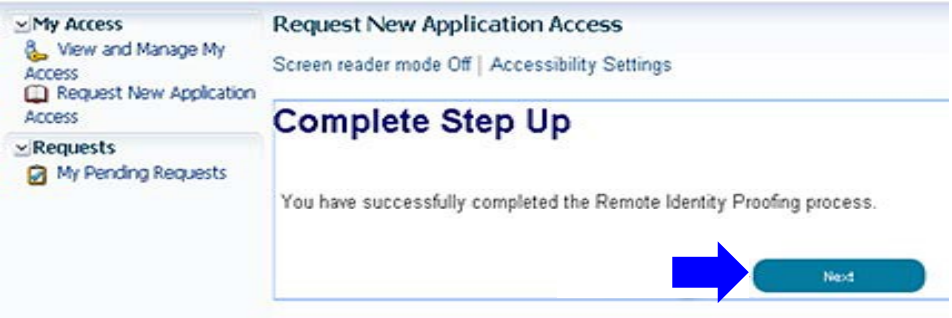


13. If the Verify Identity questions were answered properly, the Remote Identify Proofing (RIDP) process is now complete. Select [Next] to continue with the HDT User role request process, as illustrated in Figure 12.

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

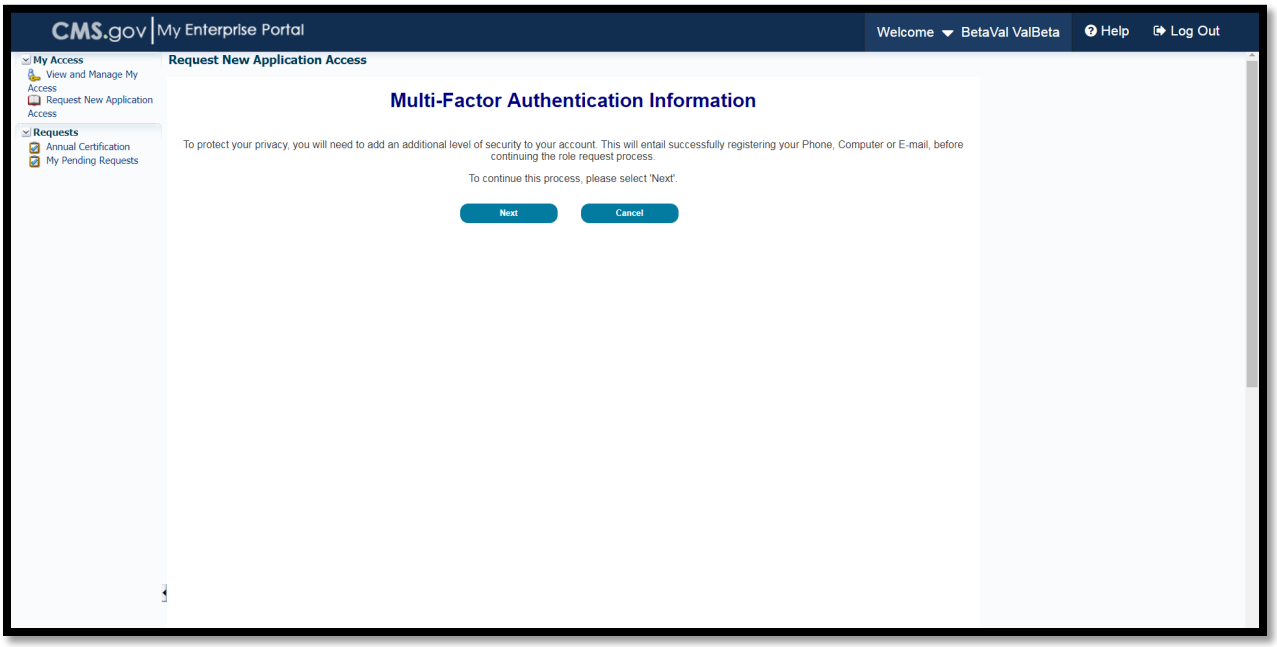
    Note: If the CMS Enterprise Portal directs you to complete the Multi-Factor Authentication (MFA) registration process now, then please refer to Section 4.3.4 for instructions.

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.

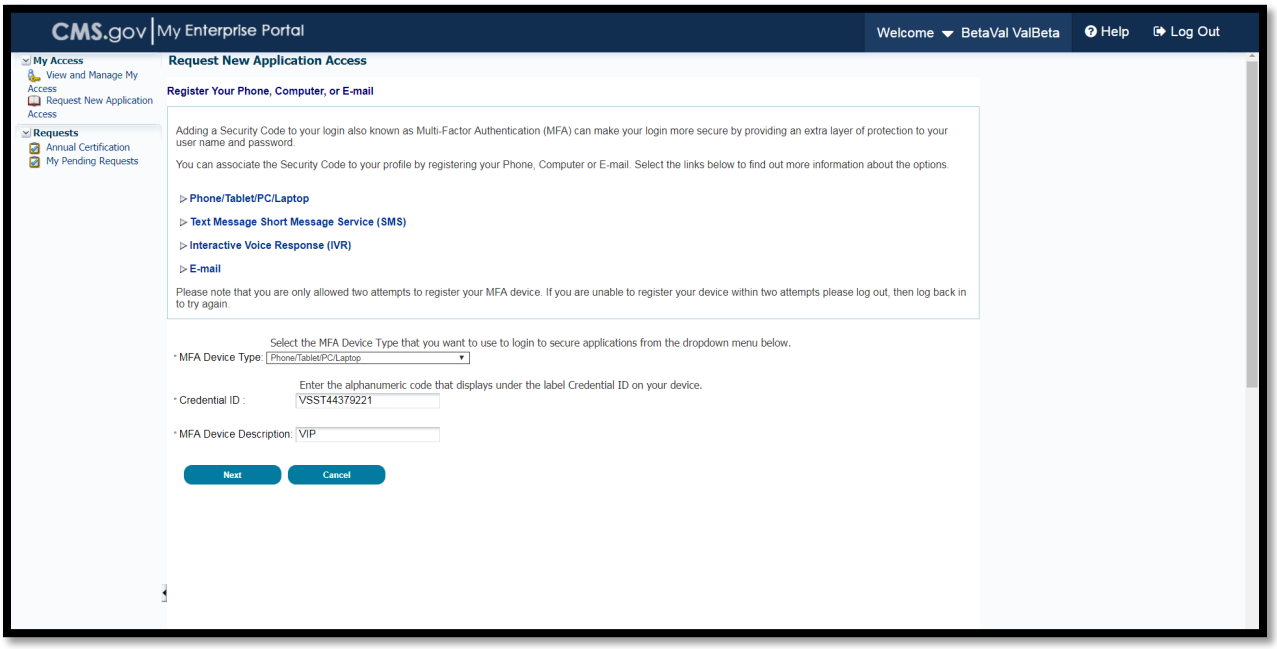
Figure 13: Multi-Factor Information Screen



1. 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] drop-down menu.

   Note: 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.

Figure 14: Register Your Phone, Computer or Email Screen

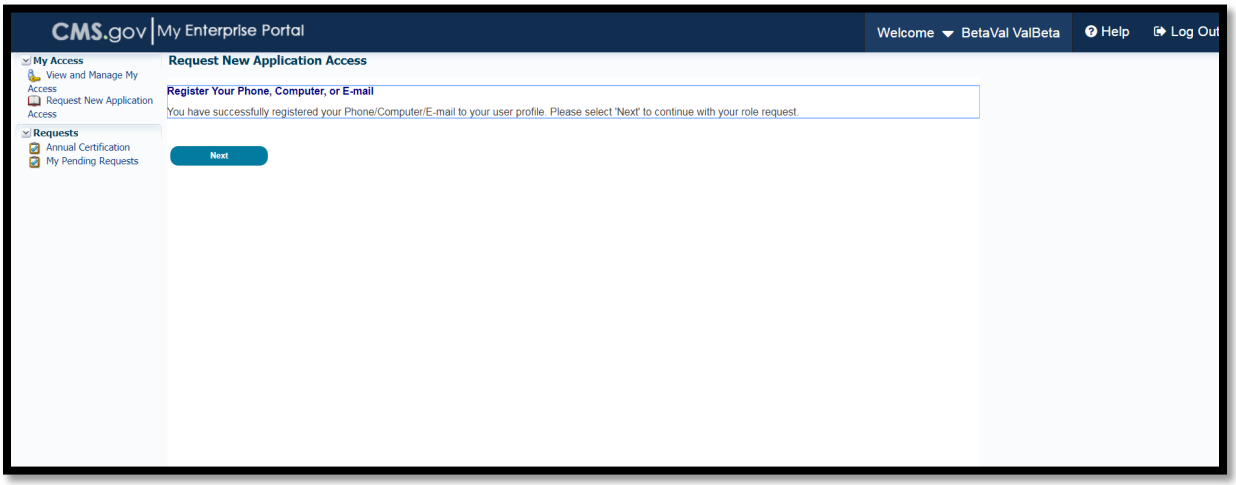


After selecting your Multi-Factor Device Type, Select [Next] to continue.

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

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

Figure 15: Complete Set Up

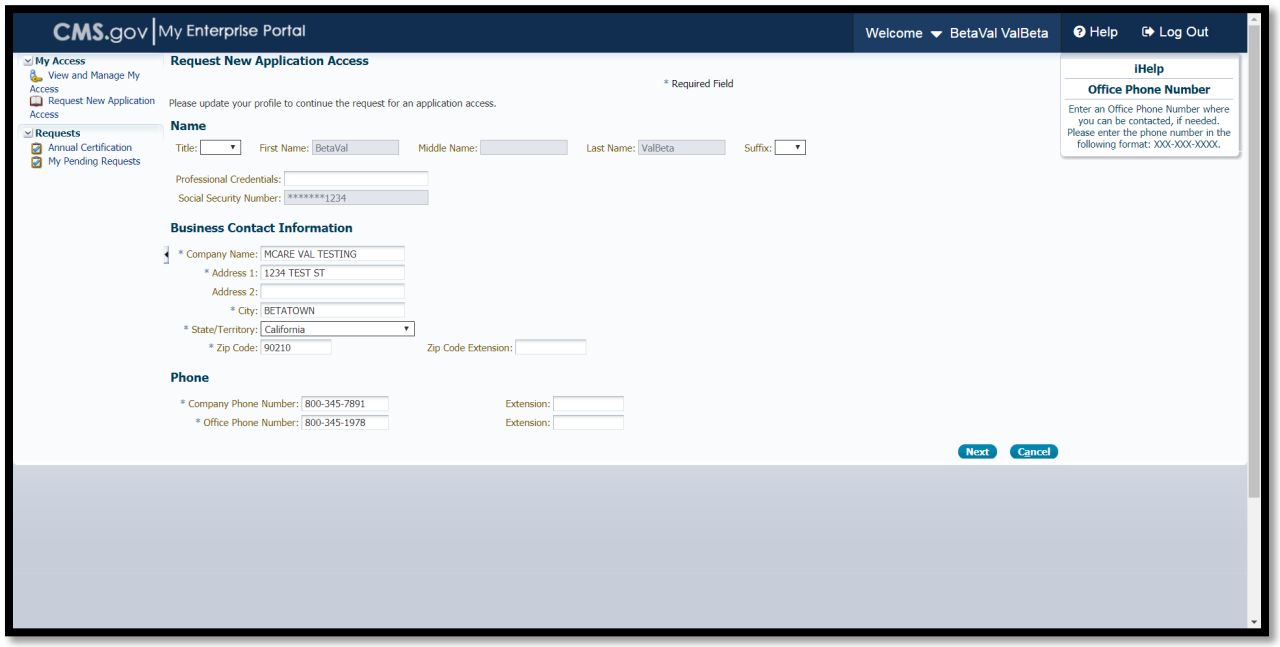


3. After completing the Multi-Factor Registration process, ***Request New Application*** page is displayed, as illustrated in Figure 16. If all of your required business contact information is not on file, you will have to provide this information before you can continue. Required fields are

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.

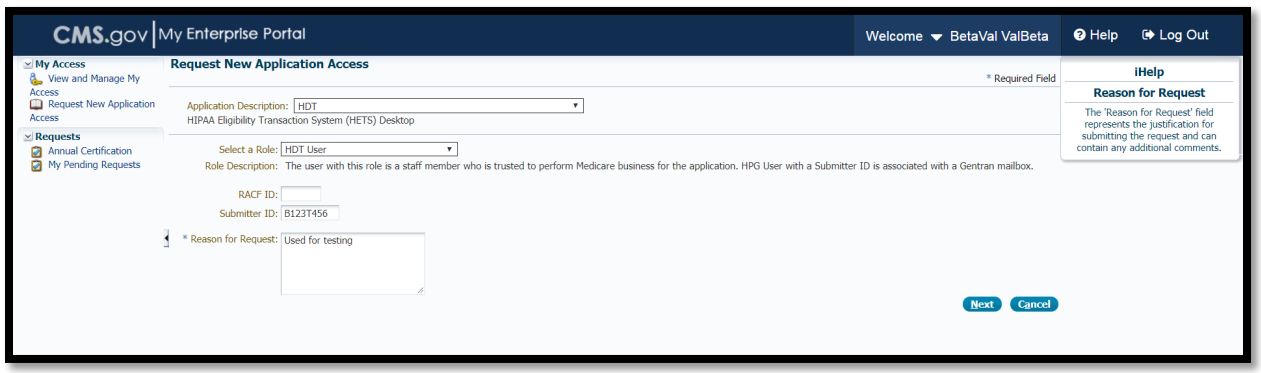
Note: If all of your business contact information is on file, the “Please update your profile…” message will not be displayed and the “Select a role” drop down menu will be displayed for you to continue. (See Step 11.) If the “Please update your profile…” message is displayed, enter the required information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

Figure 16: Request New Application Access Screen



4. 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].

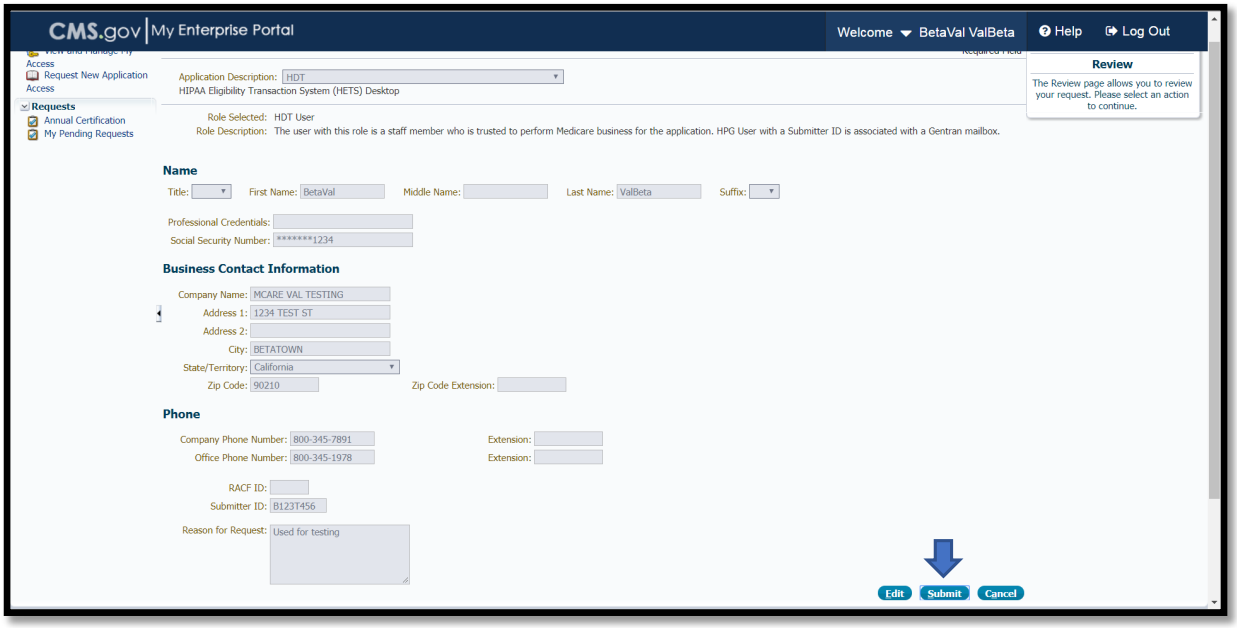
Figure 17: Provide RACF ID, Submitter ID, and Reason for Request



5. 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.

   Note: 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



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

4.3.2. CMS Enterprise Portal New User Registration

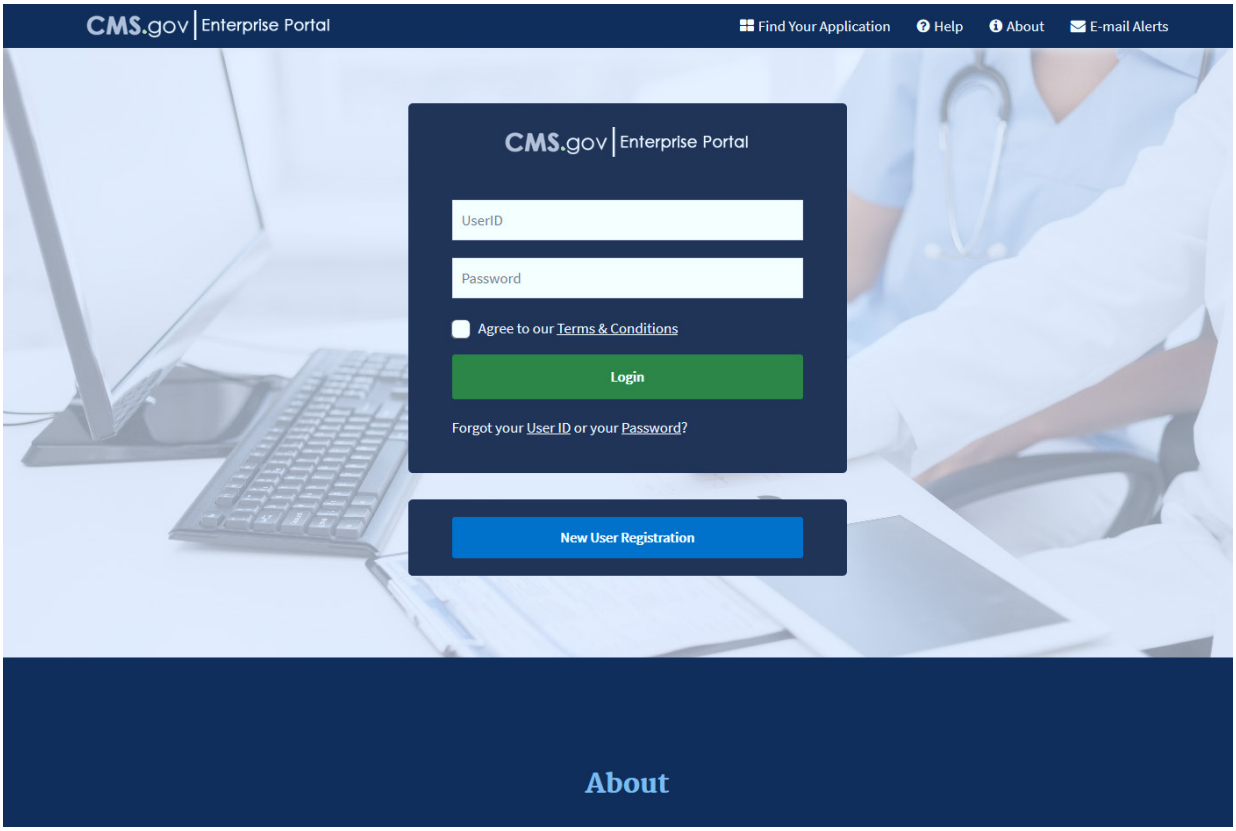
If you do not have an approved, established CMS Enterprise Portal account, you must create a new CMS Enterprise Portal account and then request to add the HDT role to that new profile. The CMS Enterprise Portal is available at https://portal.cms.gov/wps/portal/unauthportal/home/ .

Note: 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.

Note: HDT requires that all CMS Enterprise Portal User IDs be 32 alphanumeric characters or less (see Section 4.2). HDT also requires that CMS Enterprise Portal passwords contain only alphanumeric characters. Special characters such as '@', '–', '_' and '.' (dot/period) are not compatible with HDT. Please keep these constraints in mind as you create your CMS Enterprise Portal account User ID and password.

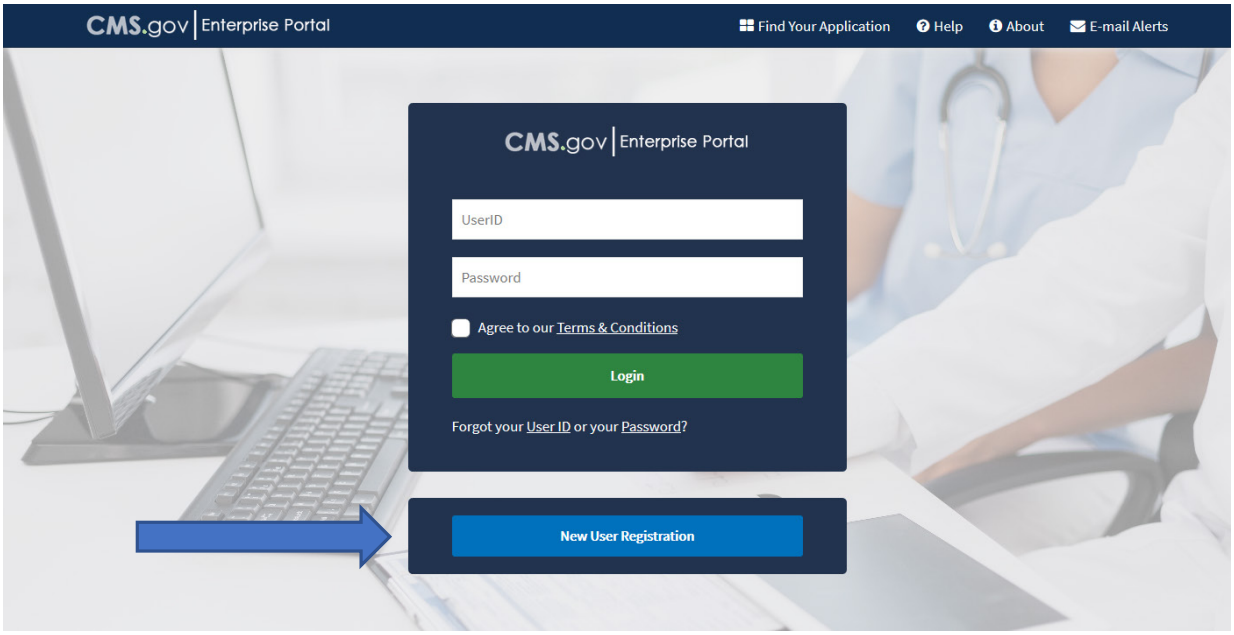
1. Navigate to https://portal.cms.gov. The ***CMS Enterprise Portal*** page is displayed, as illustrated in Figure 20.

Figure 20: CMS Enterprise Portal Screen



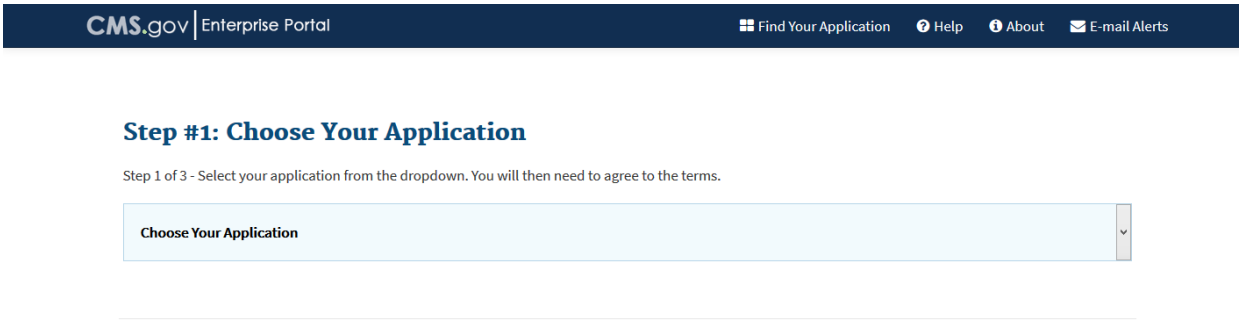
2. Select [New User Registration], as illustrated in Figure 21.

Figure 21: New User Registration



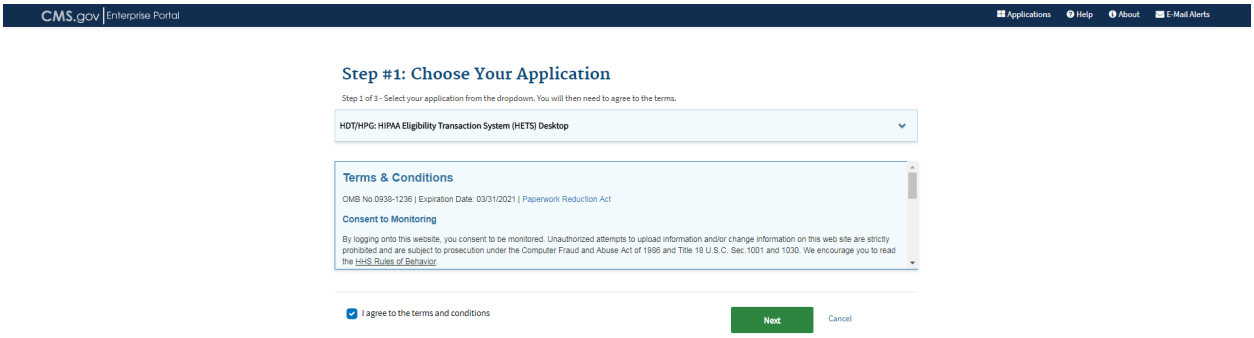
3. Select your application under the [Choose your Application] drop down. Then, as illustrated in Figure 22.

Figure 22: Choose your Application



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

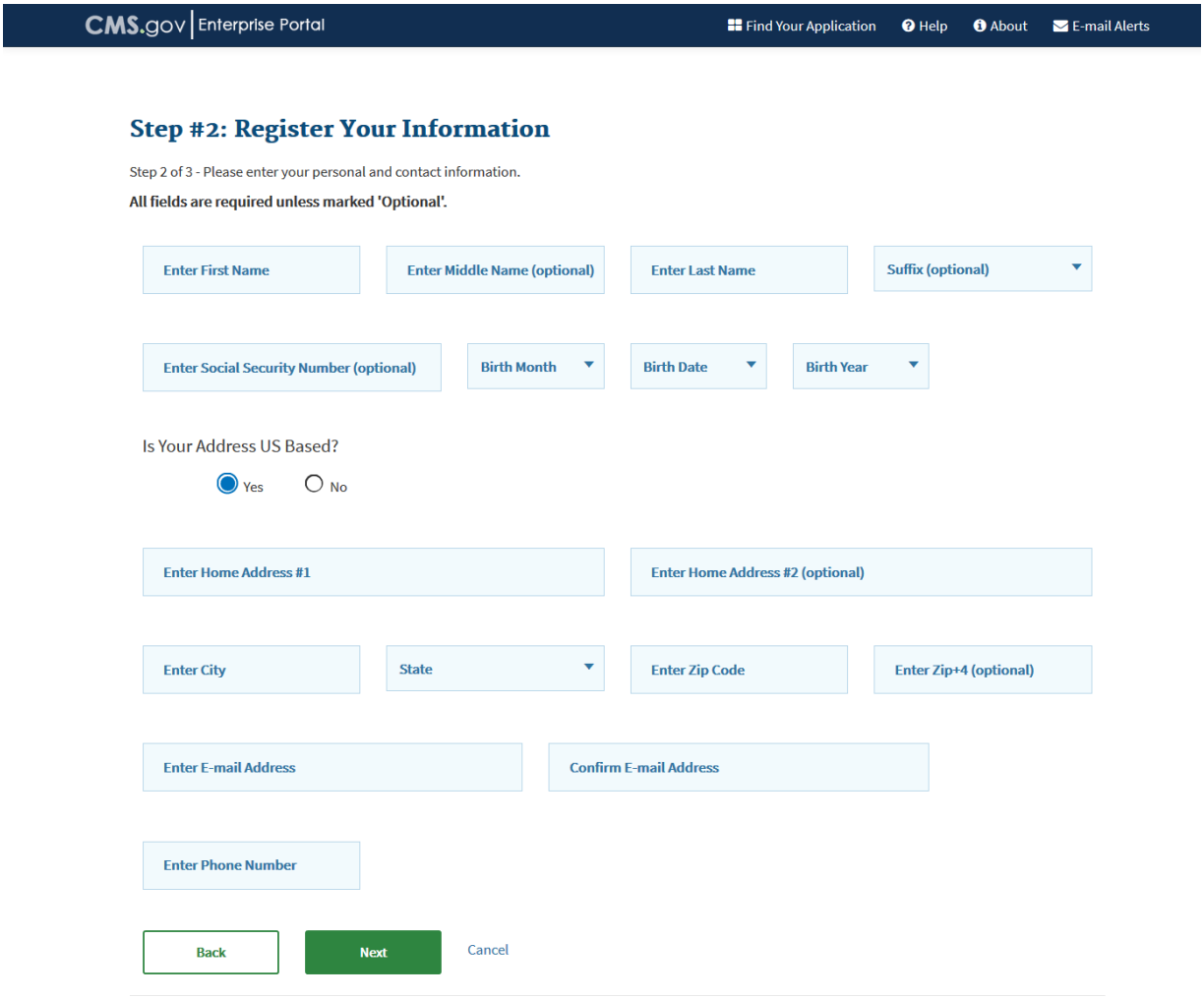
Figure 23: Terms and Conditions



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.

   Note: 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

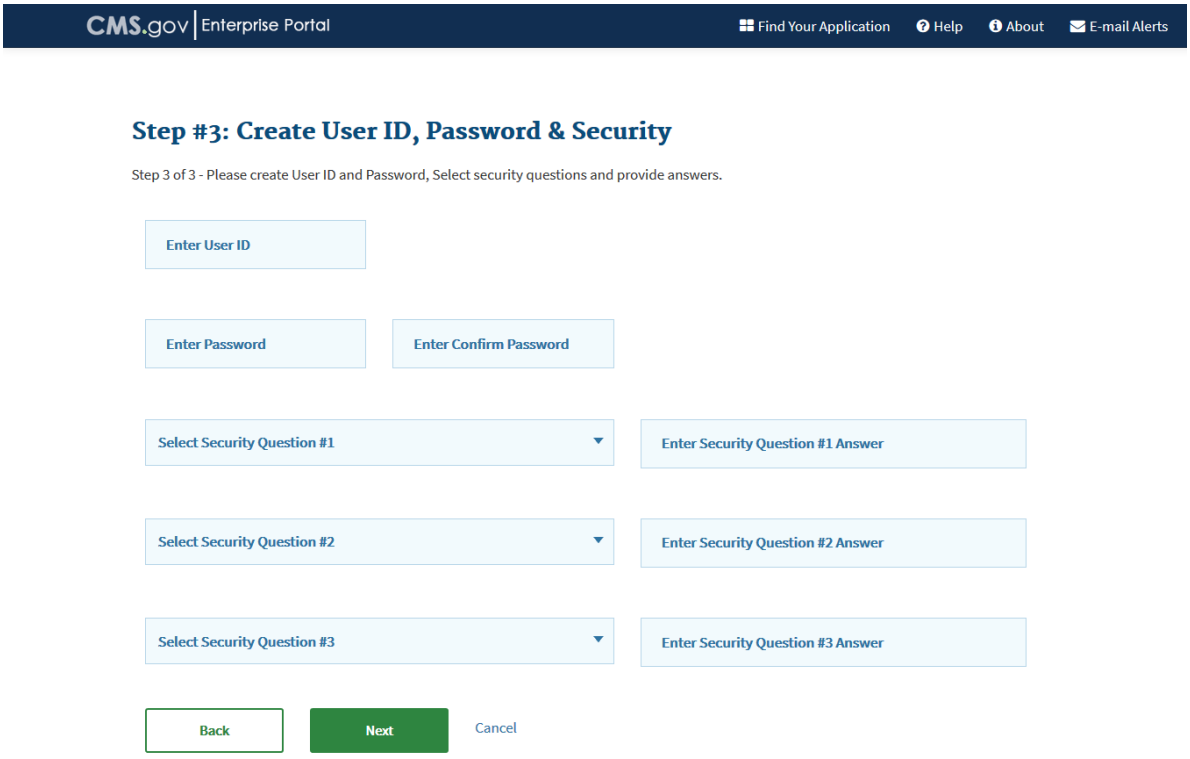


5. After providing the required information on the Register Your Information page, the Create User ID, Password & Security page is displayed, as illustrated in Figure 25. Create and enter a [User ID] of your choice and based on the requirements for creating a User ID.

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

   Note: Please note that HDT requires that all CMS Enterprise Portal User IDs be 32 alphanumeric characters or less and special characters such as '@', '–', '_' and '.' (dot/period) are not compatible with HDT (see Section 4.2).

Figure 25: Choose User ID and Password



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

   Note: 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: HDT requires that CMS Enterprise Portal passwords contain only alphanumeric characters. Special characters such as @, –, _ and . (dot/period) are not compatible with HDT.

   Note: The passwords must match before you can continue.

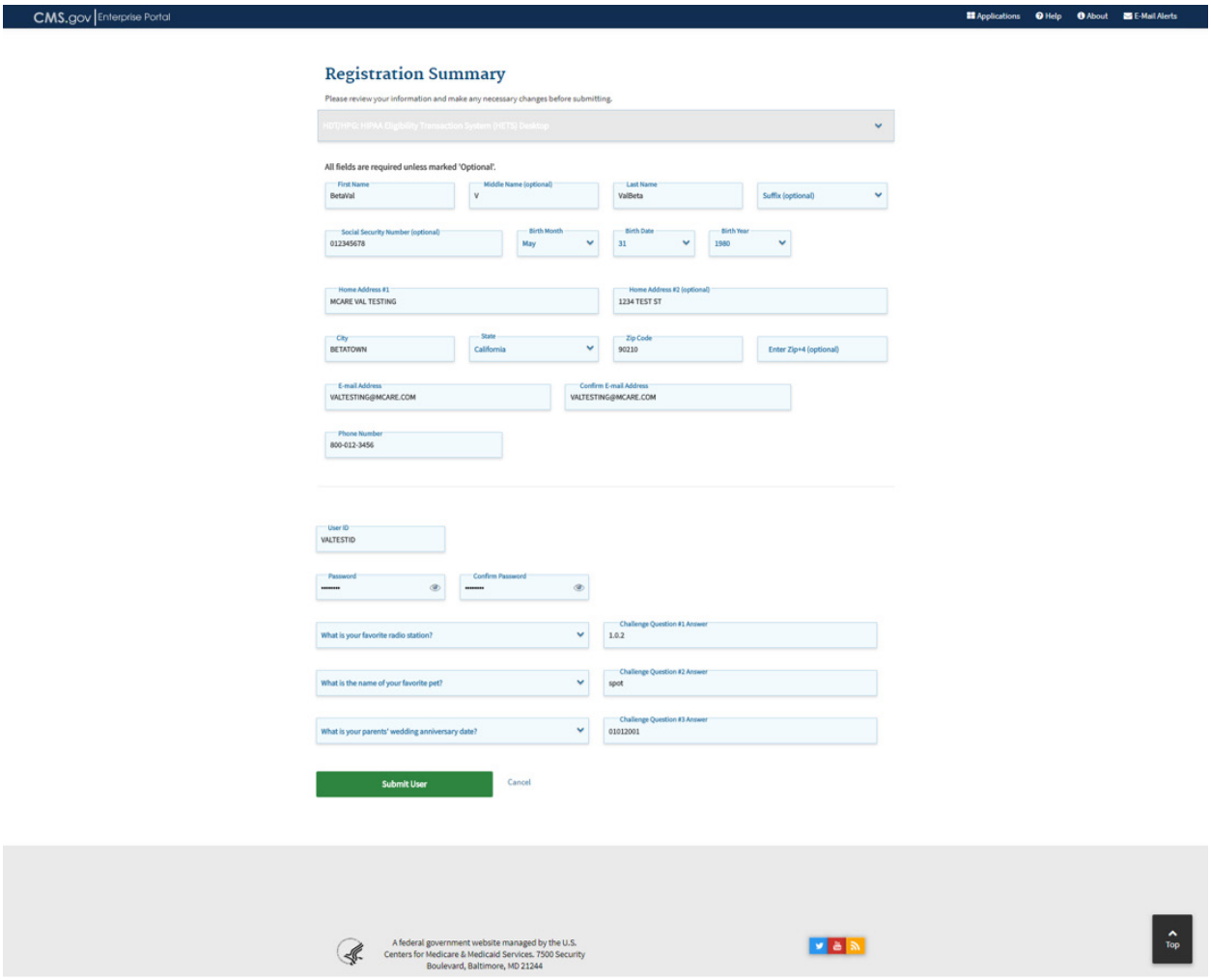
7. After entering a user created User ID and password, select a question of your choice in the [Select your Challenge Questions and Answers] section and then enter the answer you want to be saved with the question. . Continue to select a question and to enter an answer for Question 2 and Question 3.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

   Note: 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.

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

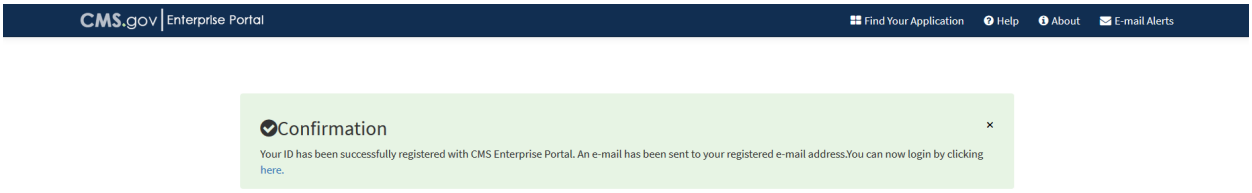
8. After selecting [Next], the ***Registration Summary*** page is displayed, as illustrated in Figure 26. The ***Registration Summary*** allows you to review the information entered for accuracy before submitting. Select [Submit User] to submit your registration request once reviewed.

Figure 26: Registration Summary



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



10. After creating your CMS Enterprise Portal User ID and password, follow the steps outlined in Section 4.3.1 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 Section 2 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 Section 2 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 Section 2 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 Section 2 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.

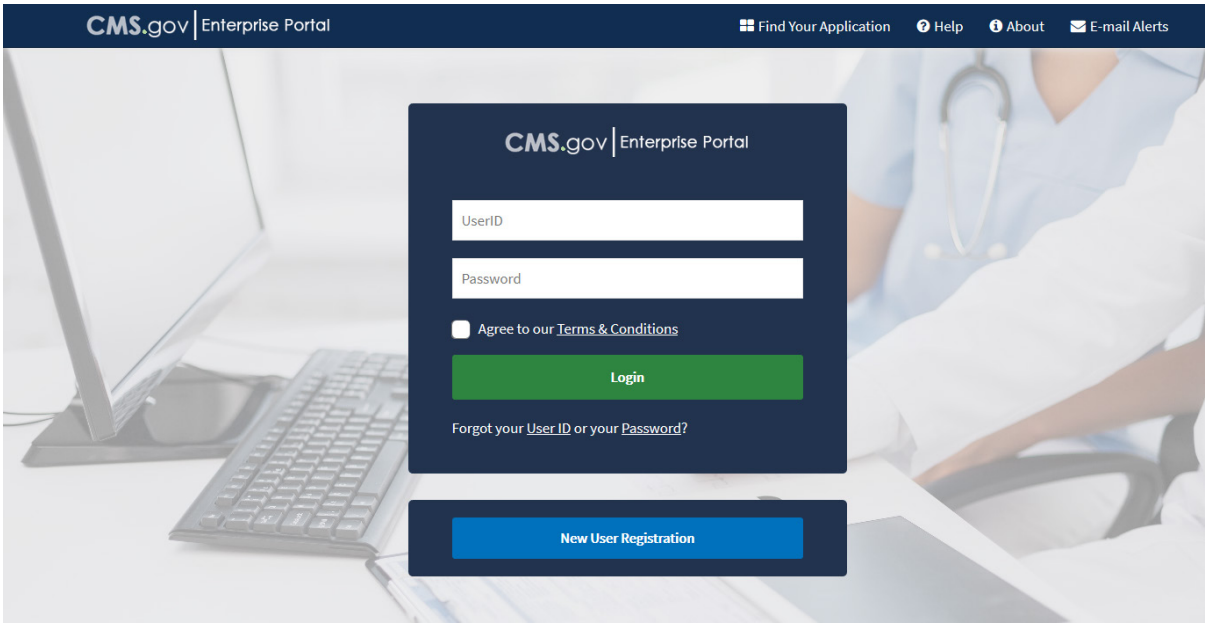
During the MFA registration process, the CMS Enterprise Portal requires registration of a phone, computer or email to add an additional level of security to a User's account. The User is given five options to select from to complete the registration process. The same steps can be followed to register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

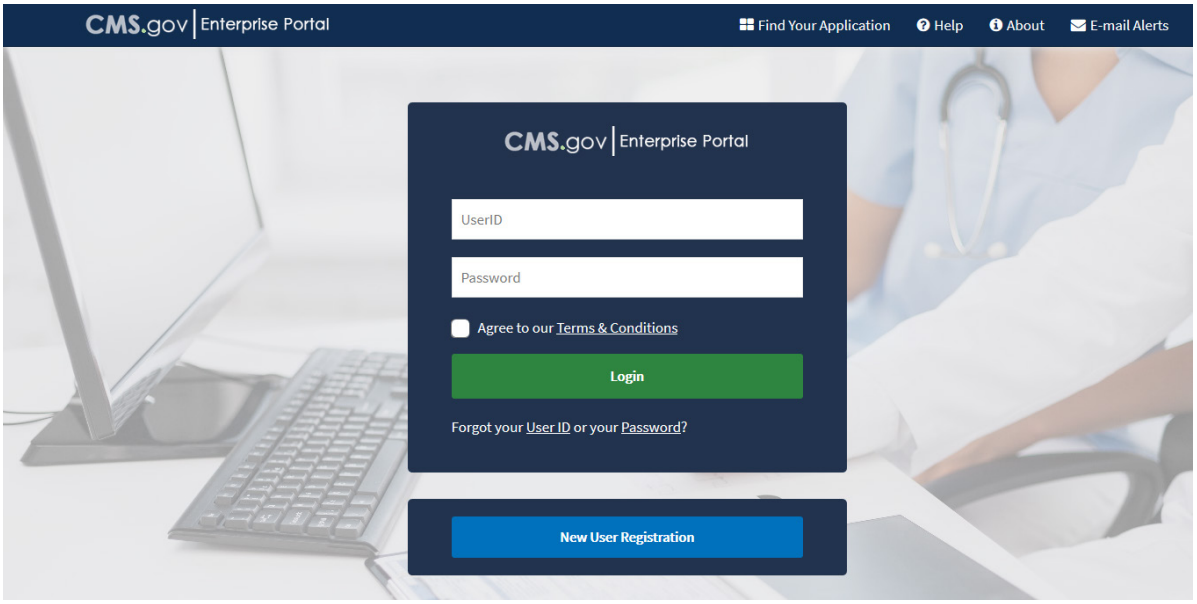
1. Navigate to https://portal.cms.gov/. The ***CMS Enterprise Portal*** page is displayed, as illustrated in Figure 28.

Figure 28: CMS Enterprise Portal Screen



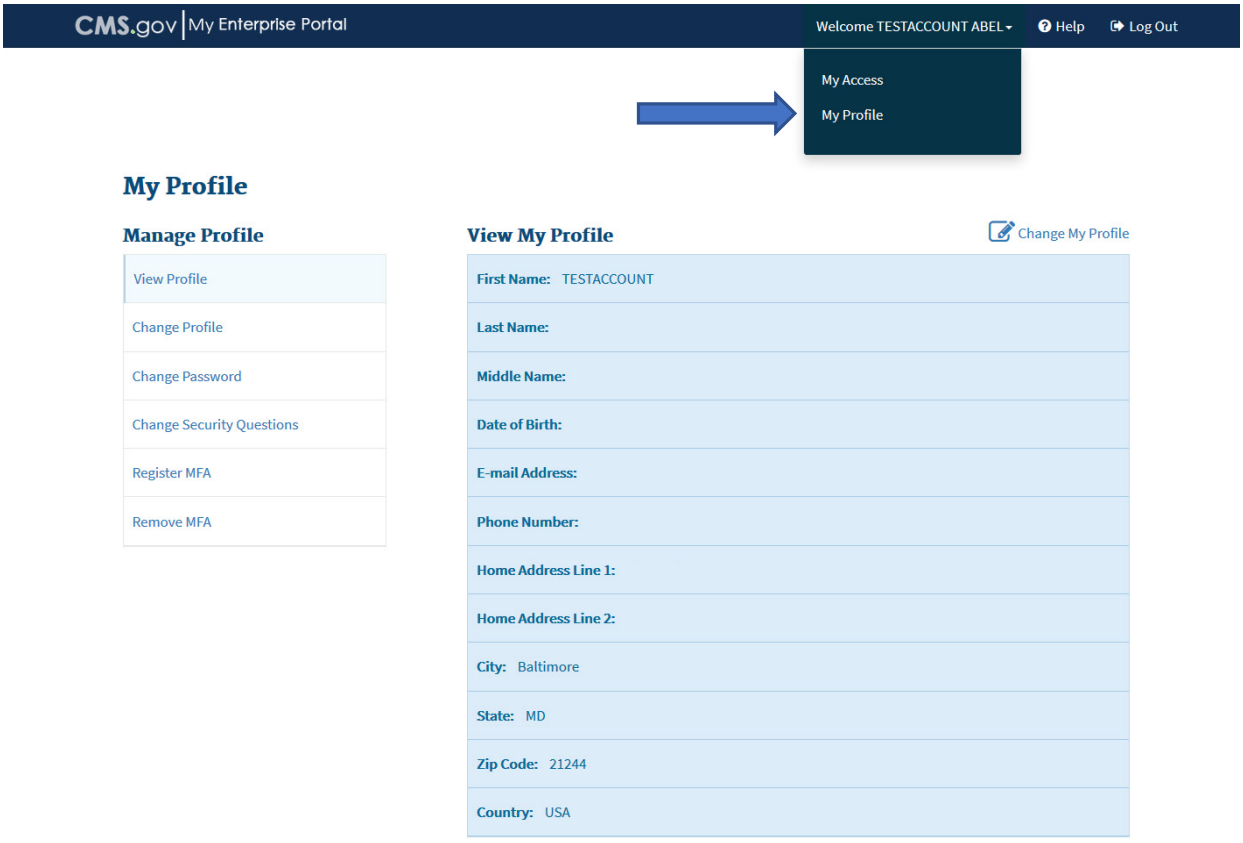
2. Enter your CMS Enterprise Portal User ID and Password, Click the [Agree to our Terms and Conditions] to continue the Registration process, then Login, as illustrated in Figure 29.

Figure 29: Login to CMS Enterprise Portal



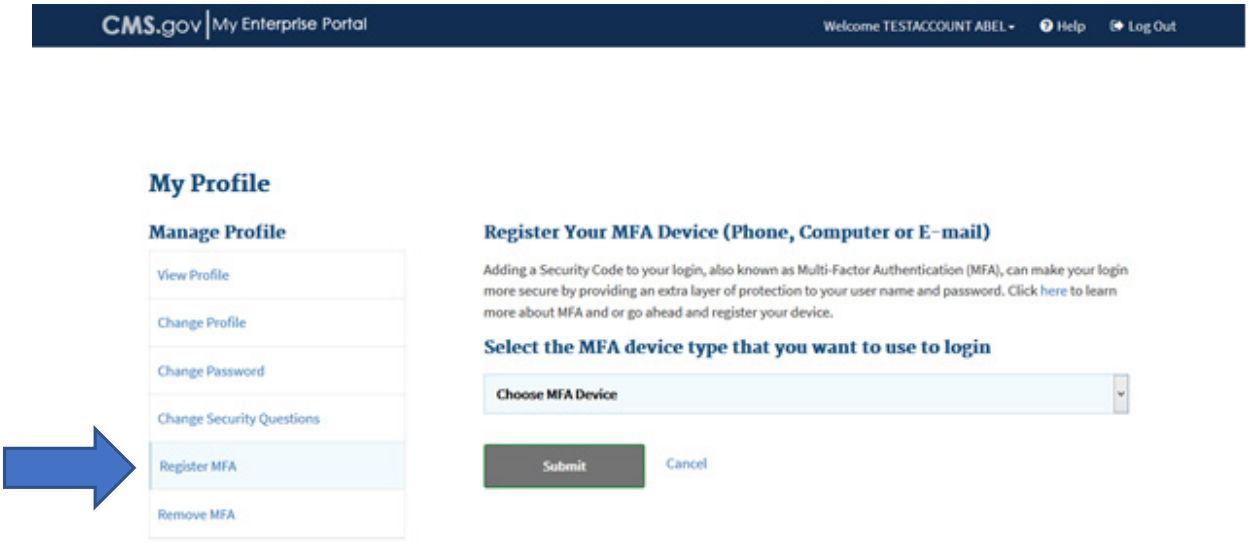
3. Select your username and then select [My Profile] from the dropdown menu to go to your profile, as illustrated in Figure 30.

Figure 30: Select My Profile



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.

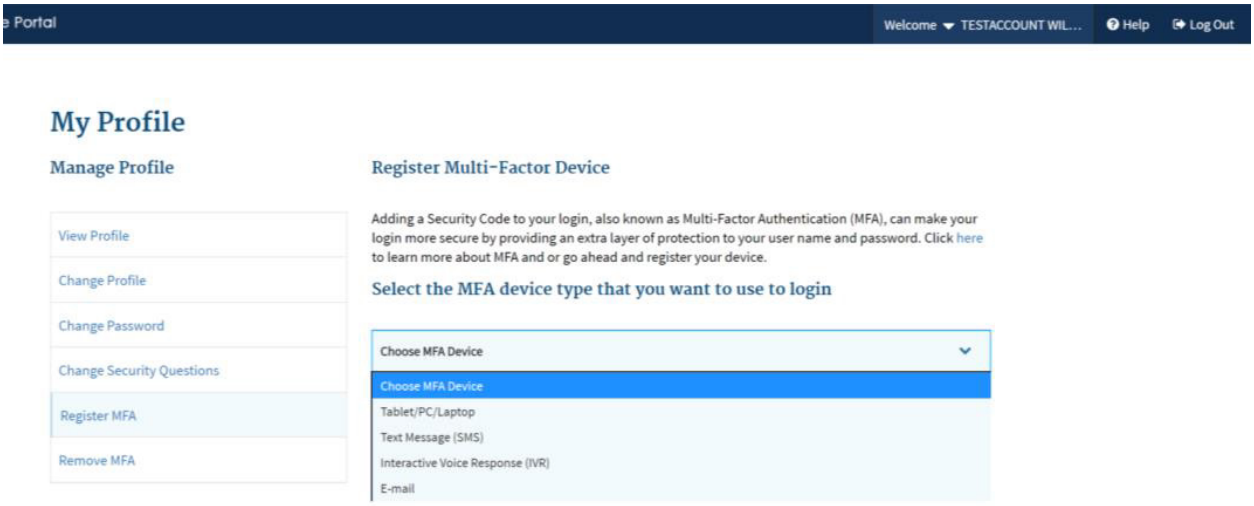
Figure 31: Register MFA



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.

   Note: 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.

Figure 32: Select Credential Type



6. (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

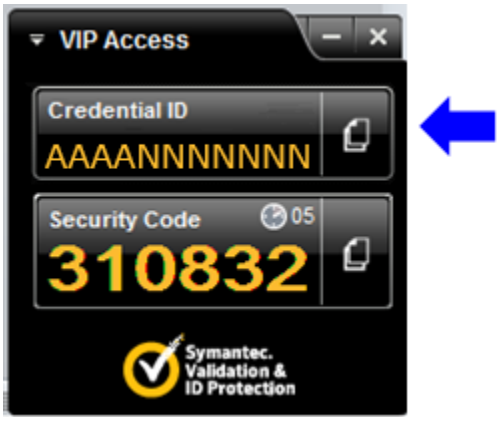
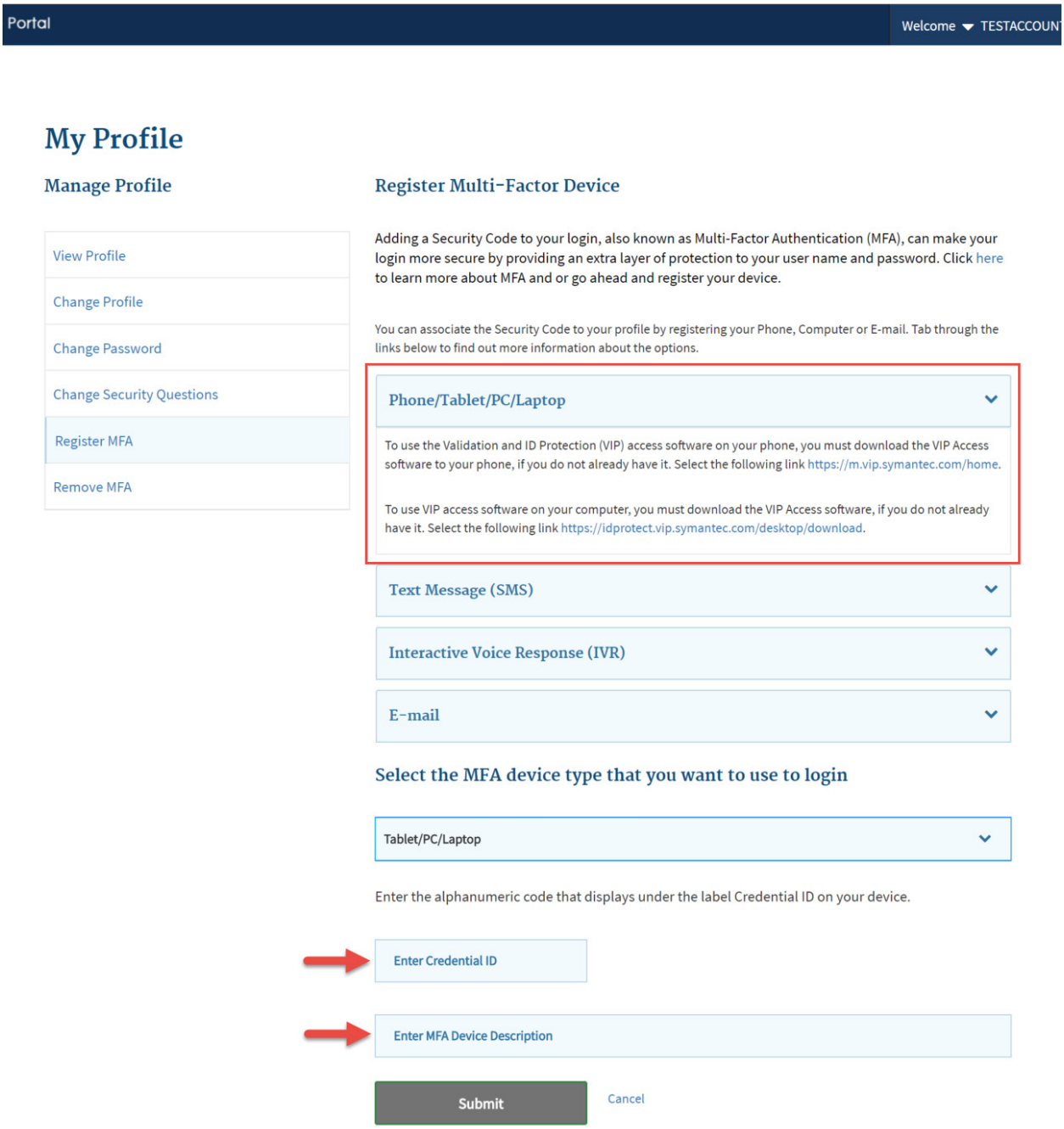
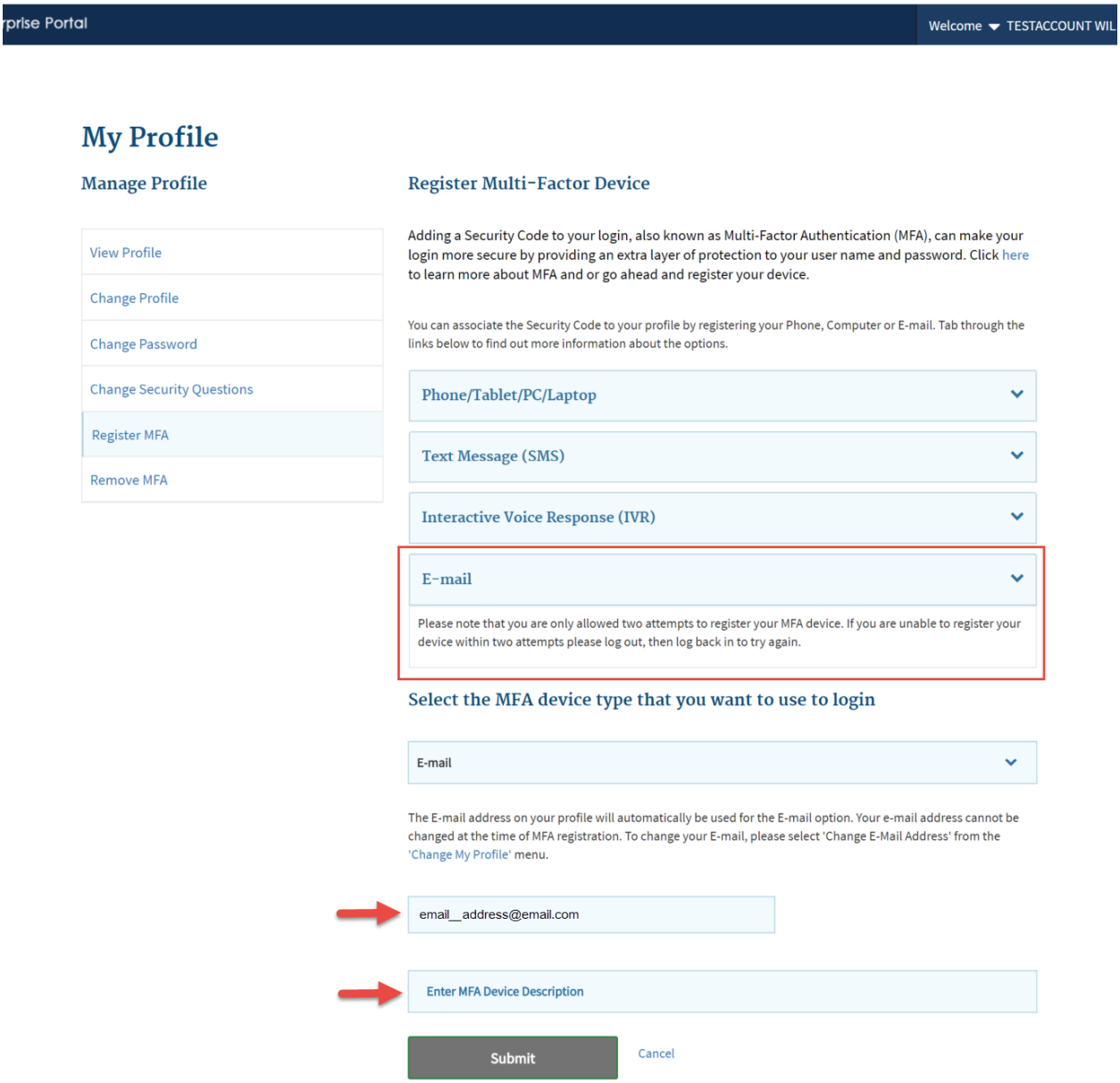


Figure 34: Select Phone/Tablet/PC/Laptop as MFA Device Type



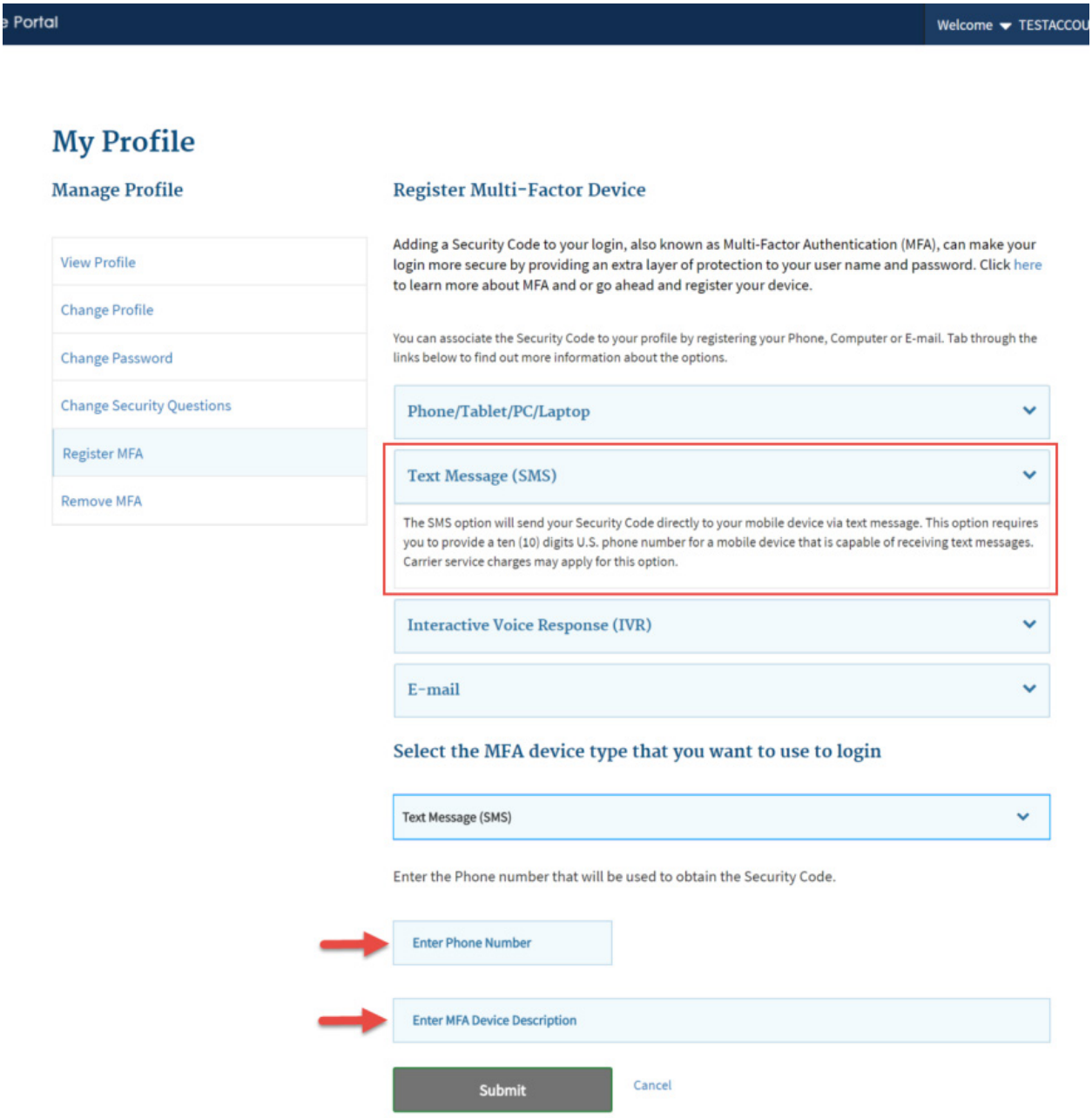
(b) Email – One Time Password (OTP). If selecting [Email – One Time Password (OTP)] as [Credential Type], the email associated with your CMS Enterprise Portal account should be entered in the field labeled [Email Address] to obtain the one time use security code. Enter [Email] as the Credential Option,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

Figure 35: Select Email as Credential Option



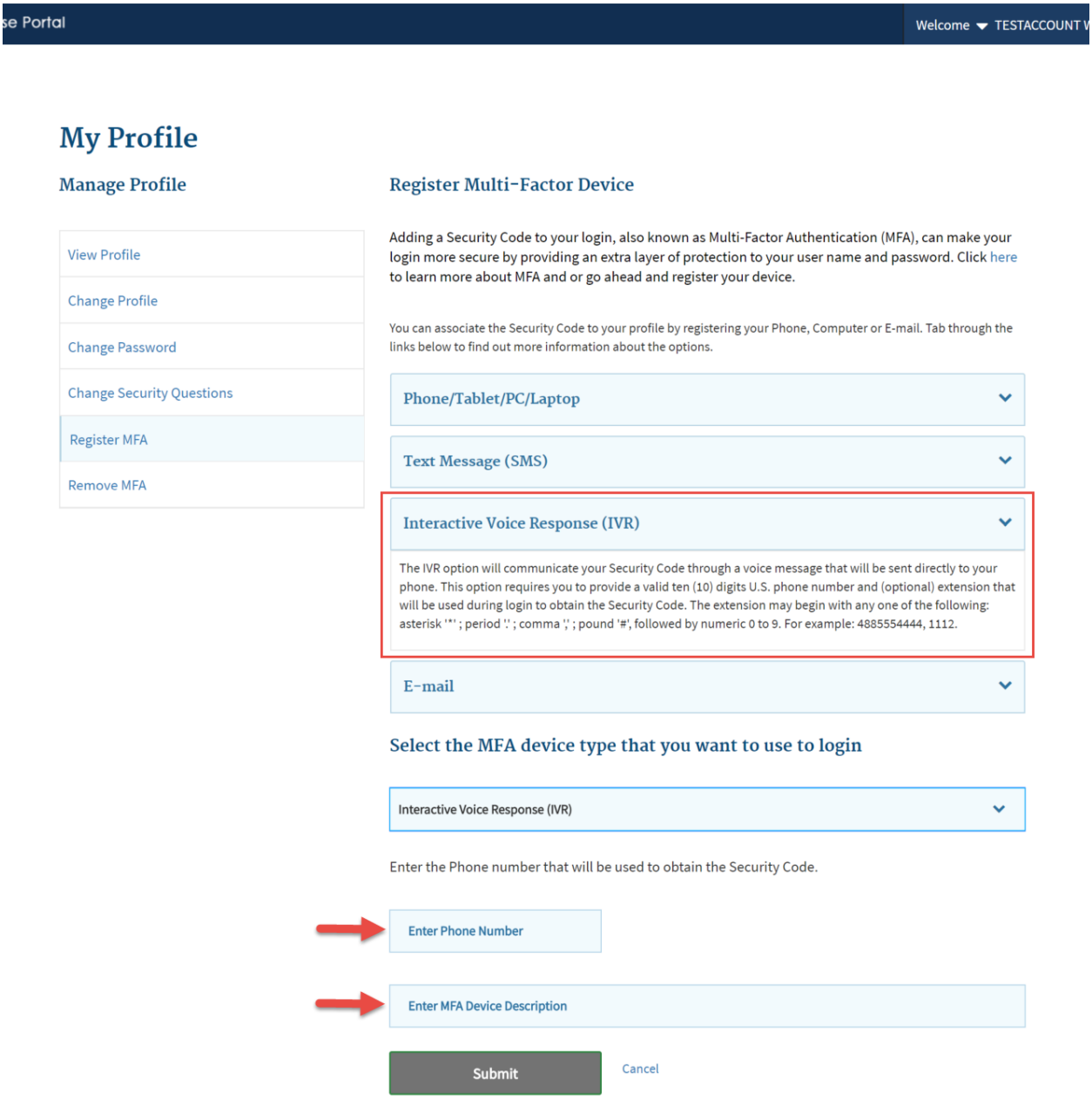
(c) Text Message – Short Message Service (SMS). If selecting [Text Message – Short Message Service (SMS)] as [Credential Type], enter the phone number that will be used to obtain the security code as [Phone Number] and [Text] as the Credential Option, as illustrated in Figure 36.

Figure 36: Select Text as Credential Option



(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

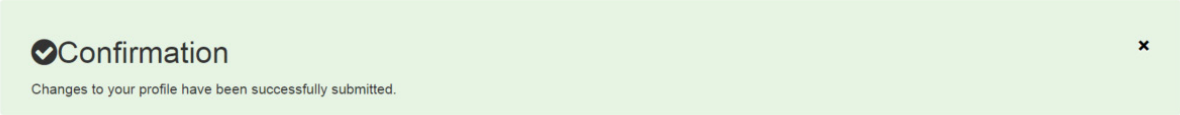


Select [Submit] to continue.

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.

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

Figure 38: Register MFA Device- Successful Confirmation Screen

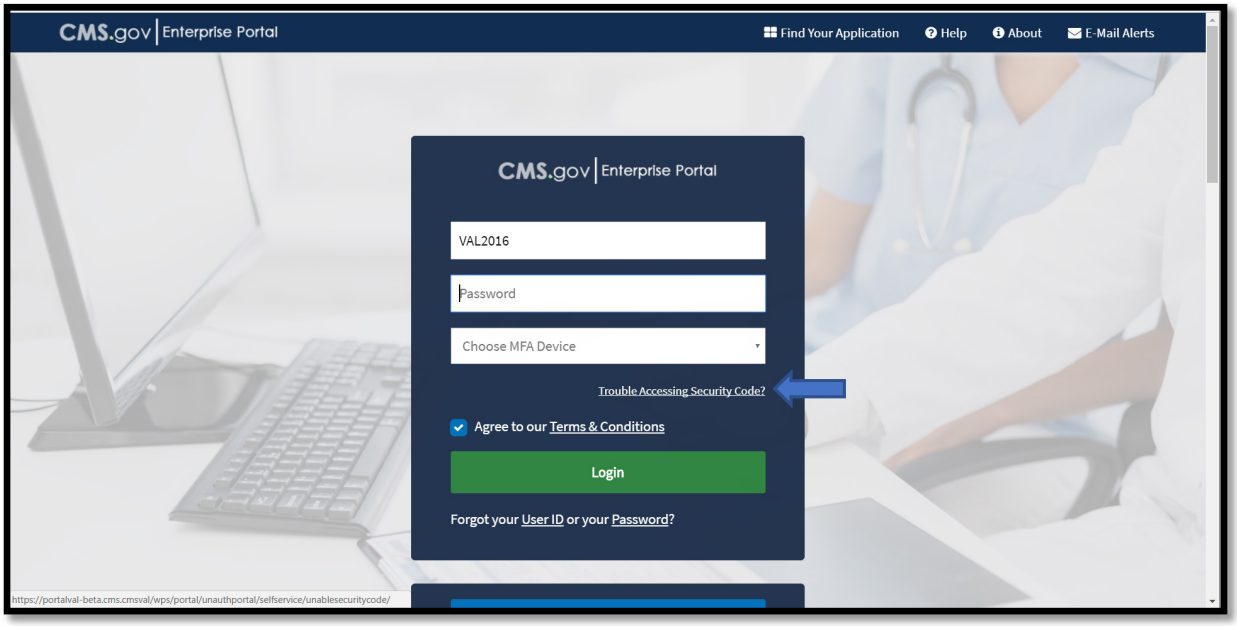


4.3.4.2. Utilizing a Security Code When the User Does Not Have Access to Their Registered MFA Device

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 Section 4.3.6. 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



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

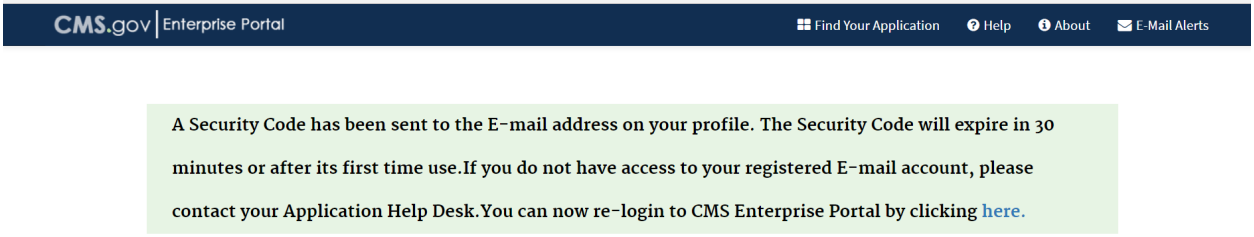
Figure 40: Unable to Access Security Code User ID Entry

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

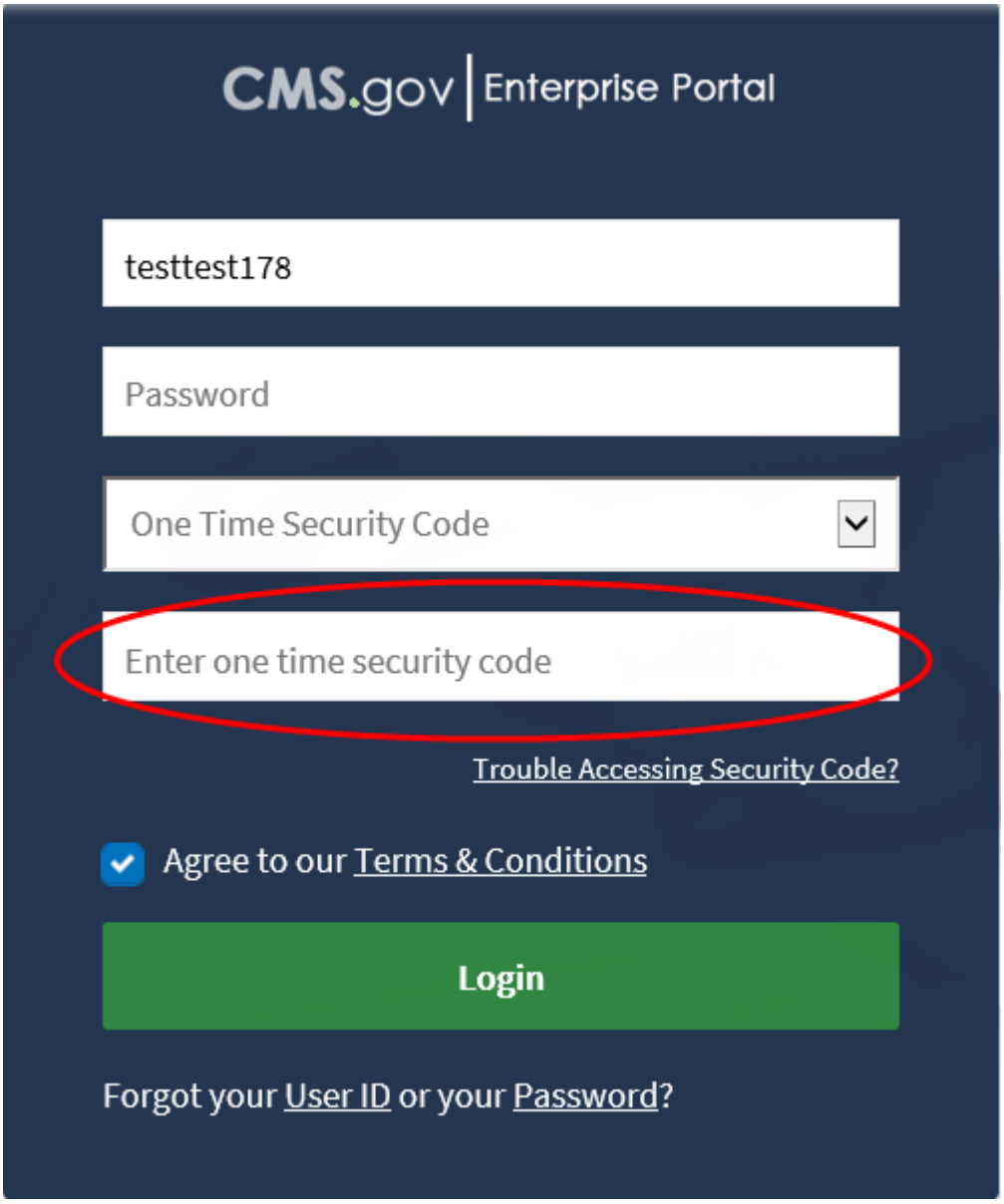
4. The User validates his/her identity by completing the challenge questions, using the answers created when the account was created. Select [Submit] to continue. The Unable to Access Security Code self-service process is completed, as illustrated in Figure 42. The CMS Enterprise Portal will send a Security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

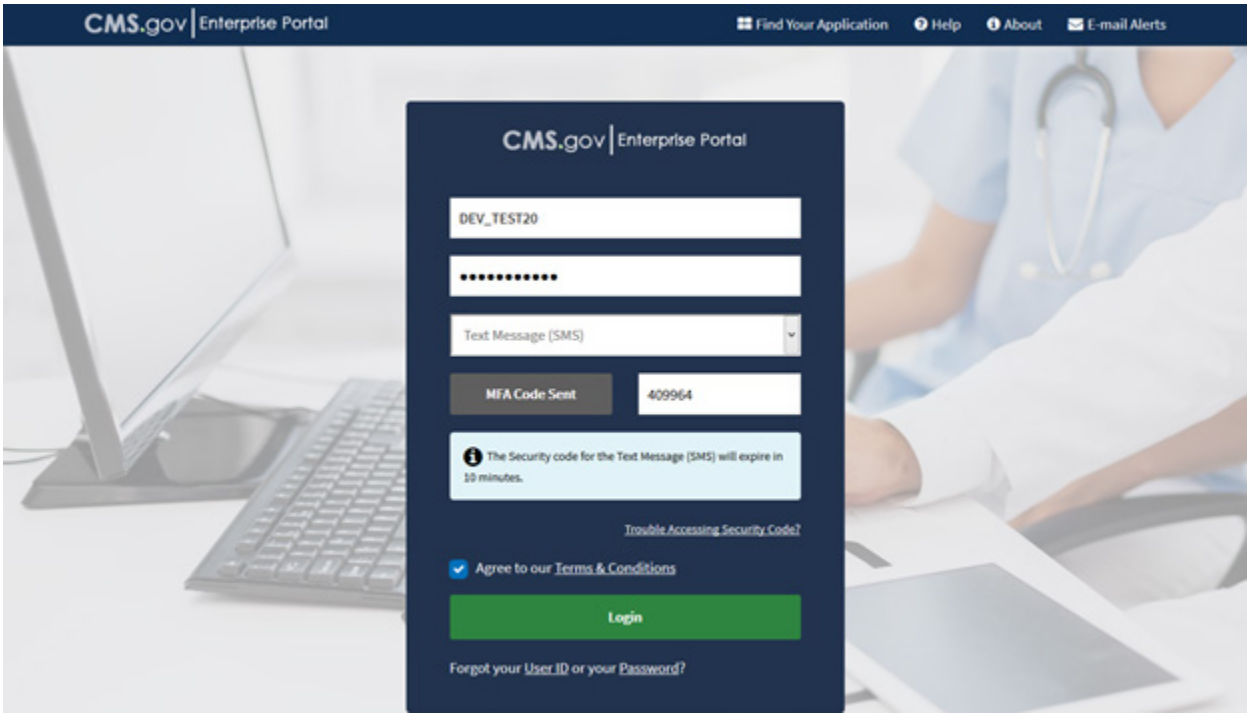


4.3.4.3. Removing a Registered MFA Device

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

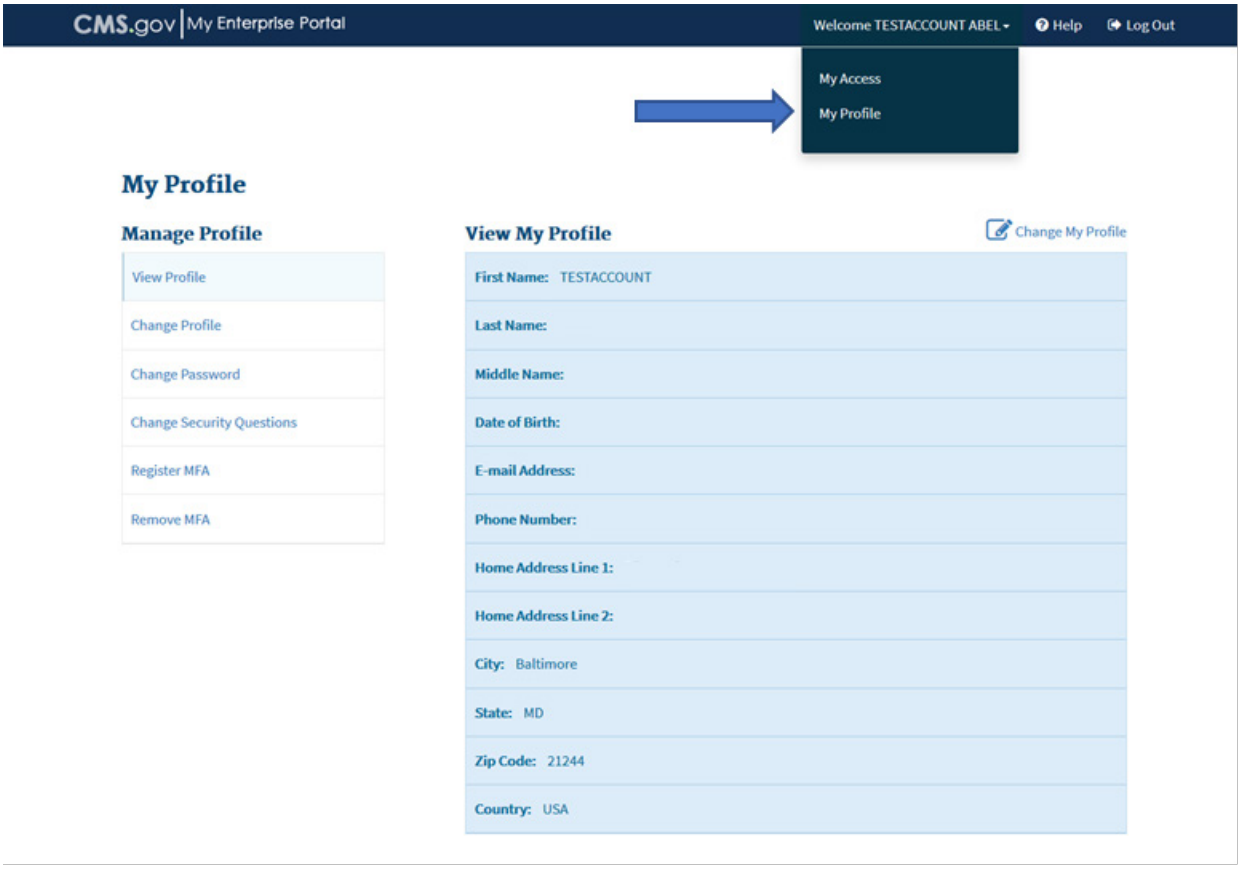
1. Navigate to https://portal.cms.gov/. The ***CMS Enterprise Portal*** page is displayed, as illustrated in Figure 44.

Figure 44: CMS Enterprise Portal Screen



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.
3. 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

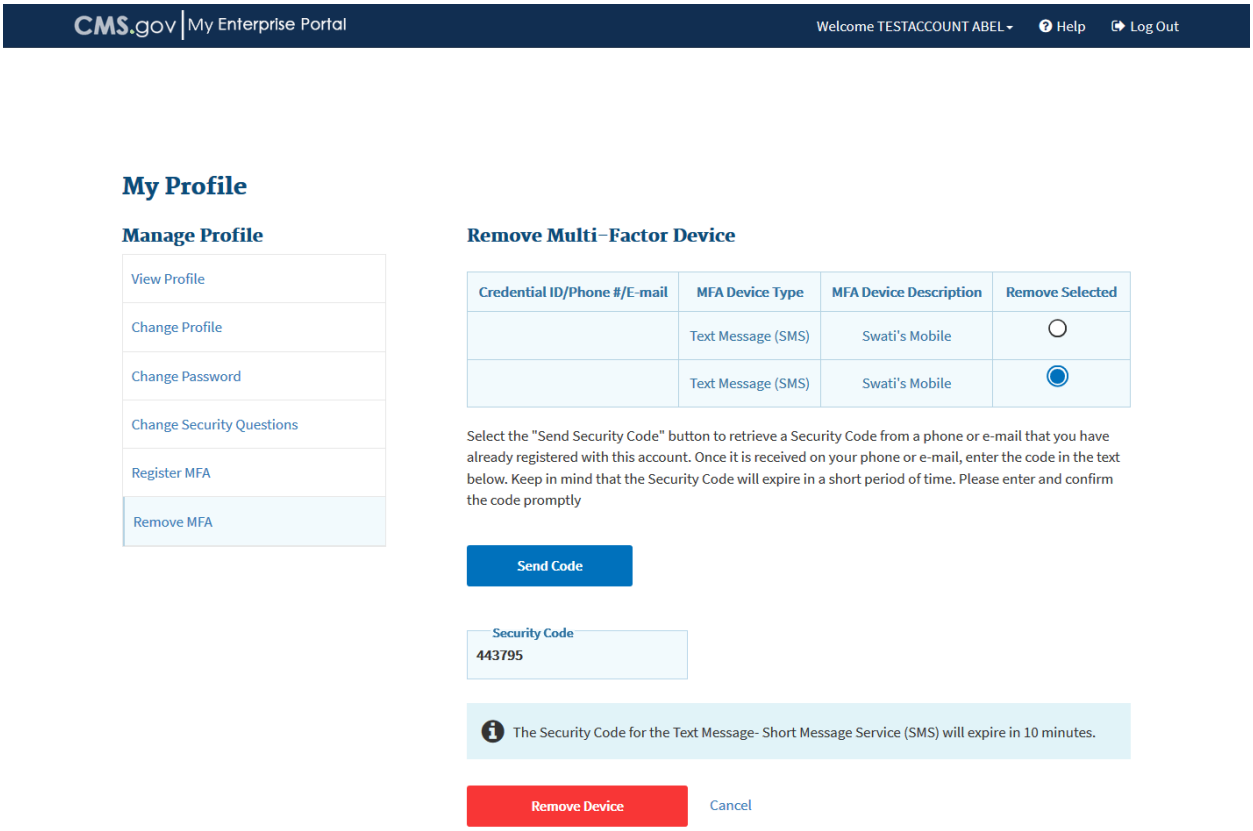


5. Select [Remove MFA] from the left navigation links to begin the process of removing an MFA device from your account, as illustrated in Figure 46.

   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.

   Note: 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.

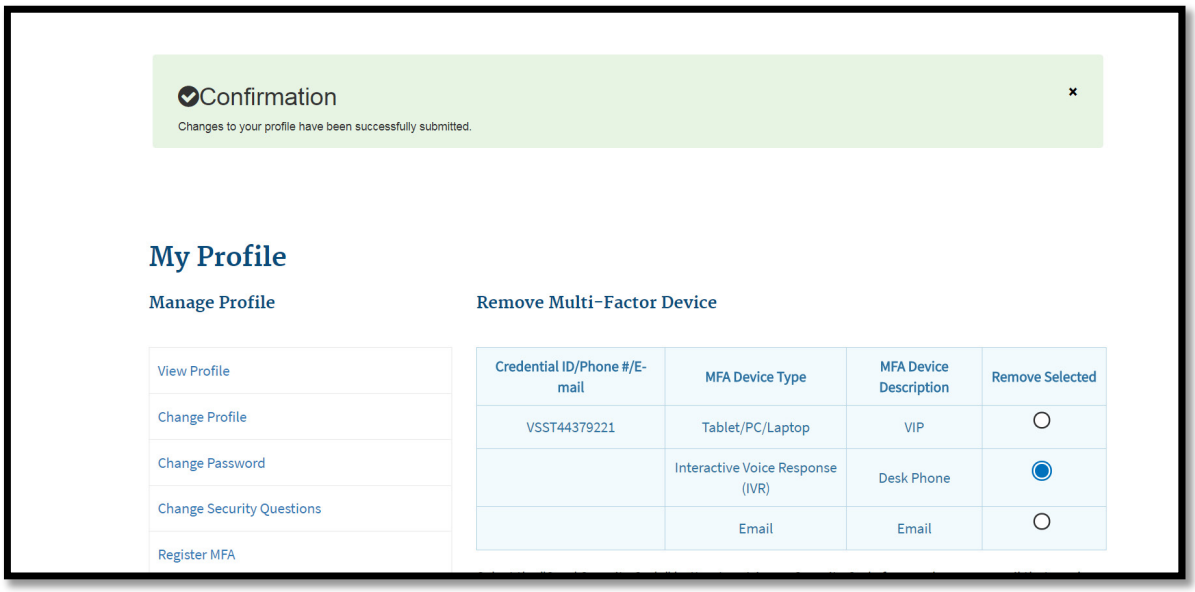
Figure 46: Remove Your Phone or Computer



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.

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

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 Section 4.3.1, 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: Experian Customer Assistance.

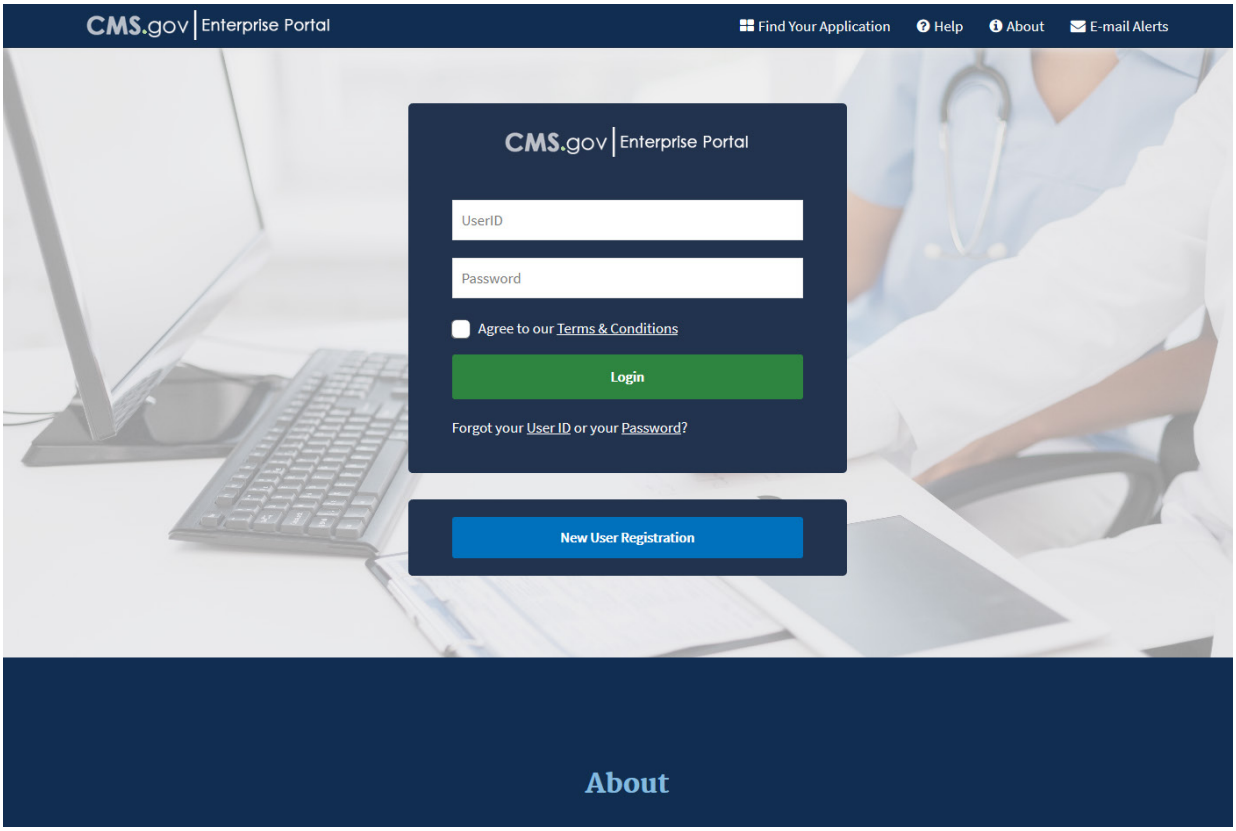
If you are asked to contact the MCARE Help Desk, you will be given a response code to help the MCARE Help Desk perform the manual identity proofing process with you. Please contact MCARE via the information provided in Section 6.5 of this guide.

4.3.6. Login to the HDT Application

Follow these steps to login to the HDT application:

1. Enter the CMS Applications Portal URL in a web browser: https://hdt.cms.gov. 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.

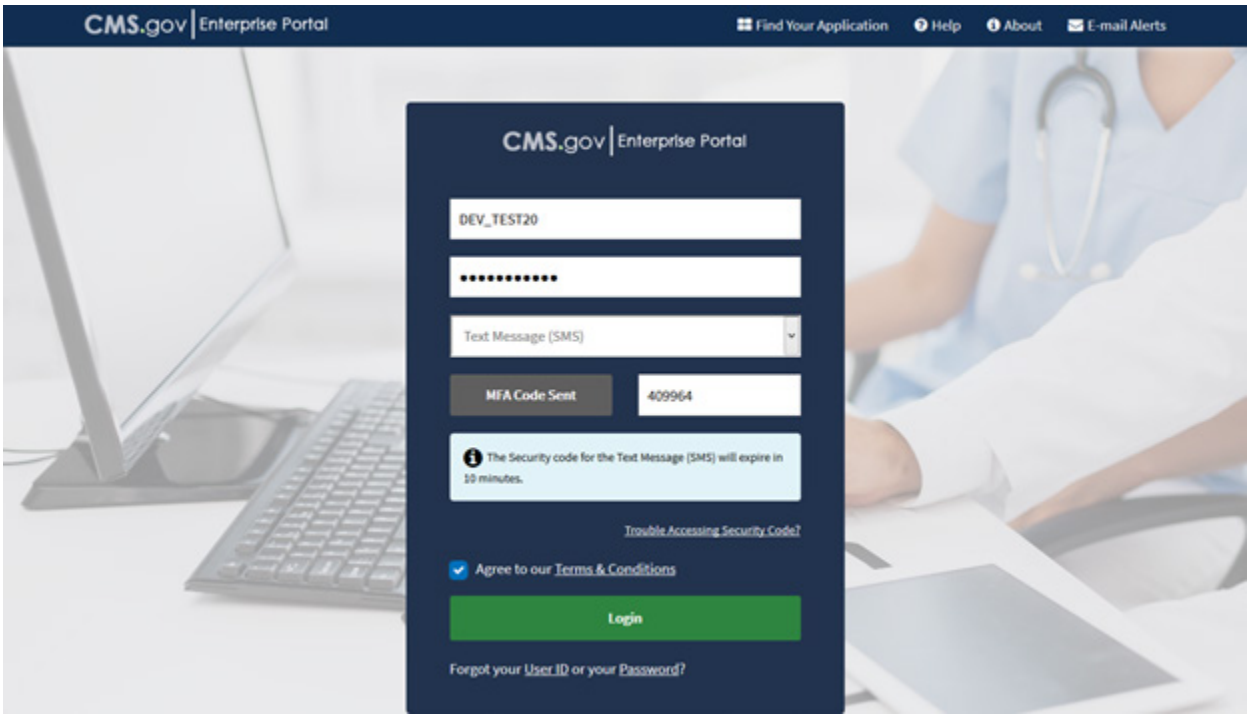
Figure 48: CMS Enterprise Portal Screen



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



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].

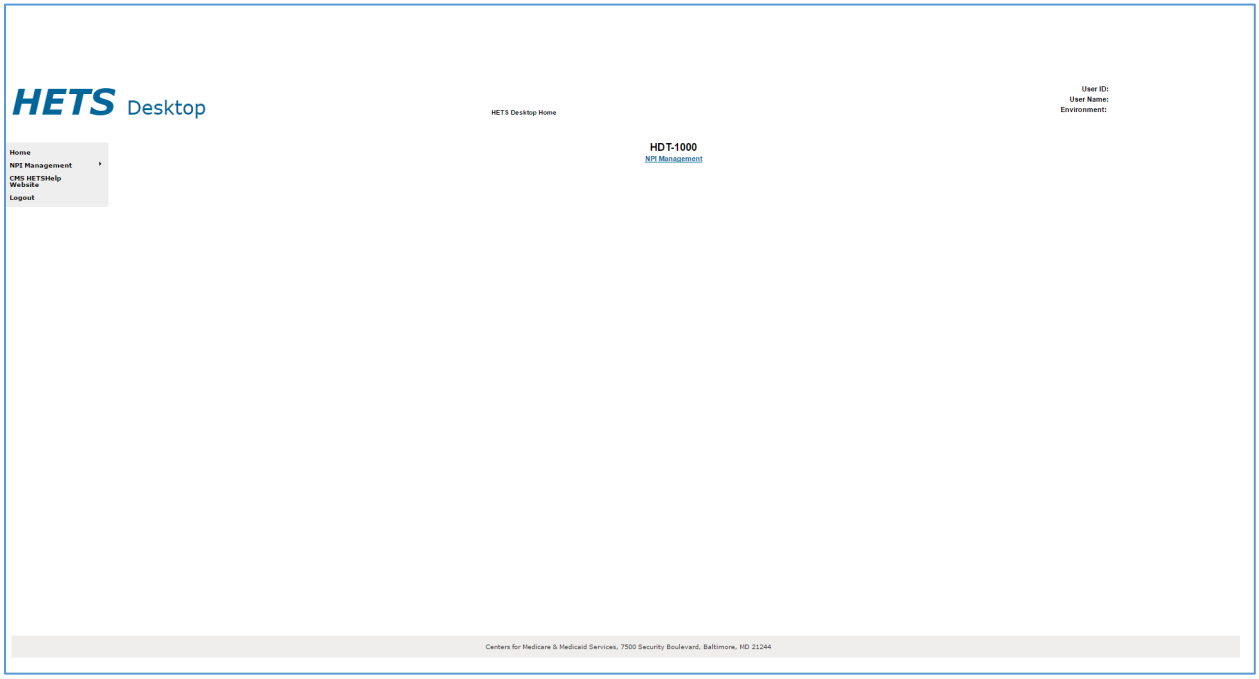
Notes:

- If you need to register a MFA Device, select the [Register MFA Device] link and complete the process described in Section 4.3.4.1.
- 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 4.3.4.2 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 Section 6.5.
- 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 Section 4.3.3.3 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)



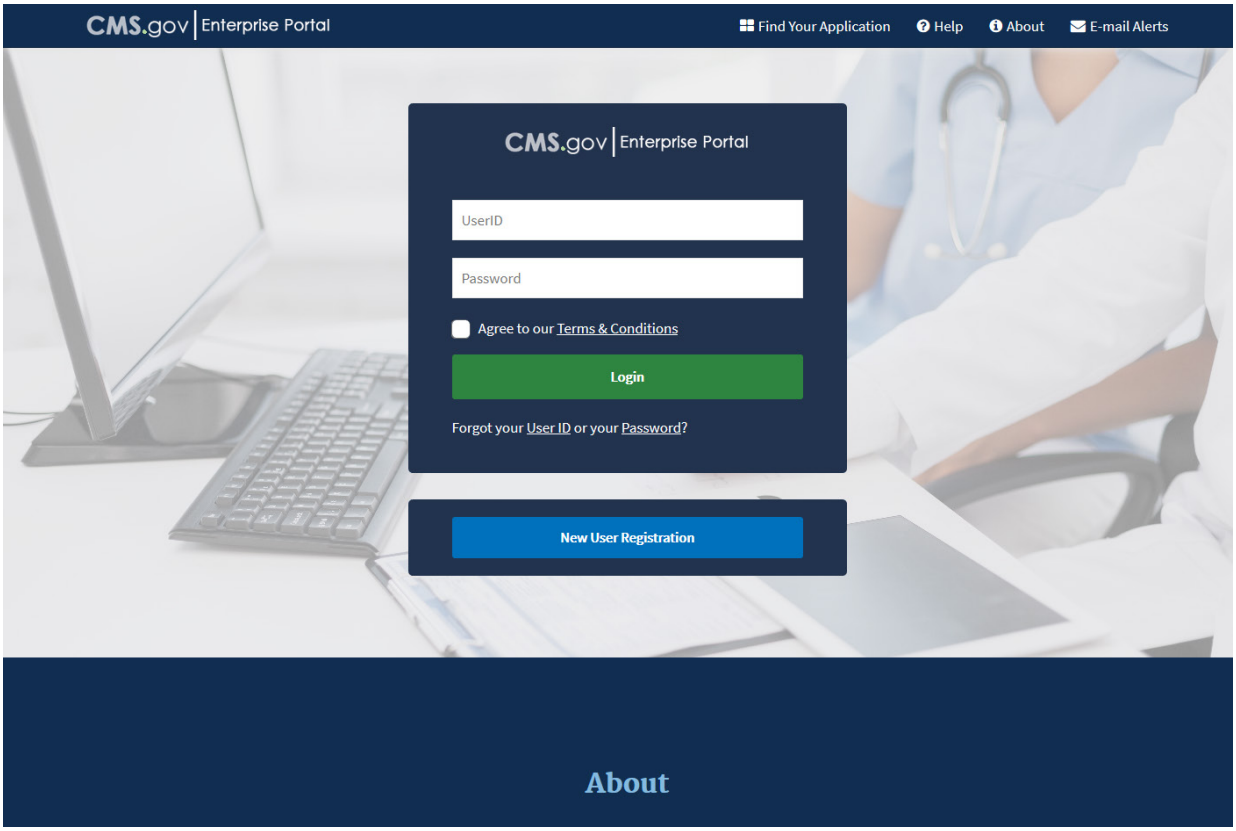
4.4. Application Organization & Navigation

Specific functionality and screen captures are described in Section 5.1 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.

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:

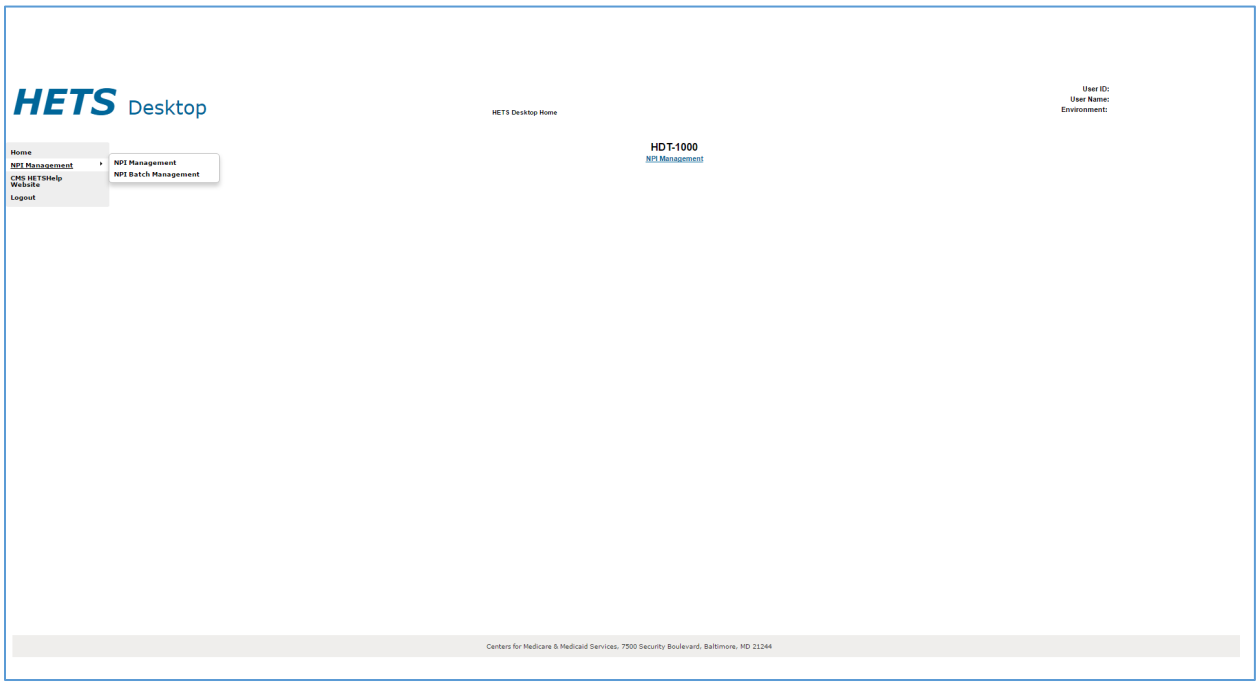
The links to navigate through the HDT application are:

- 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:

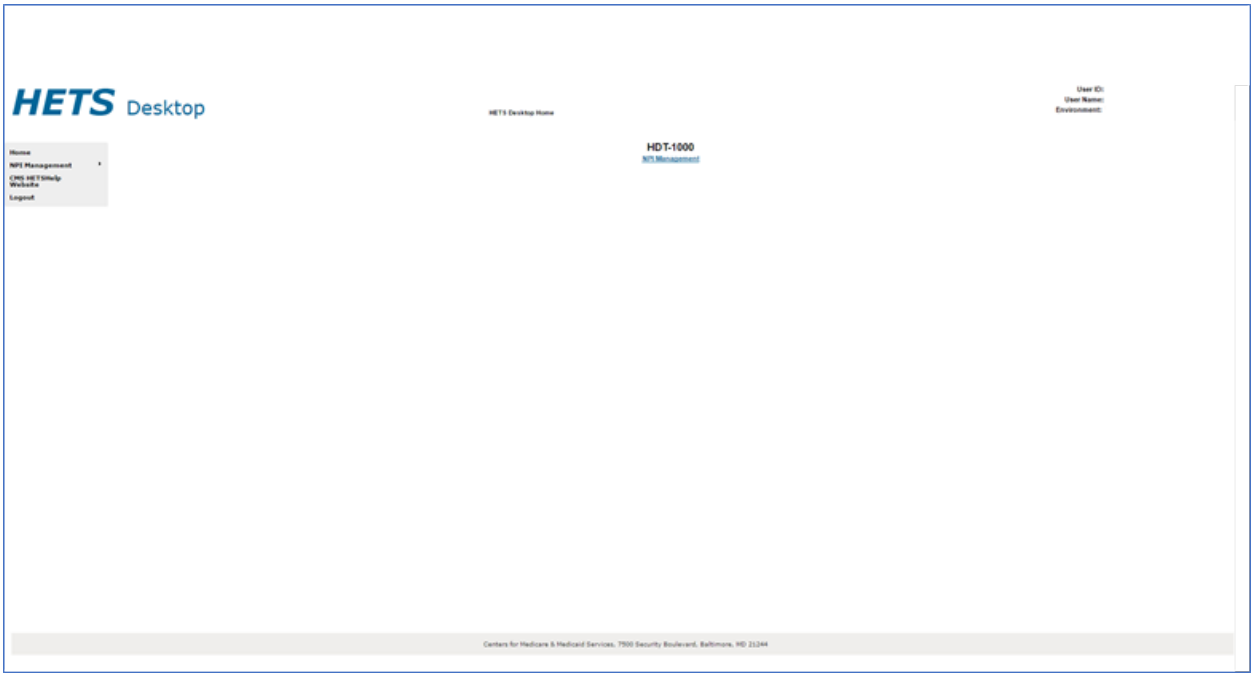
- CMS HETSHelp Website

Figure 52: HDT Application Site Map



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)



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:

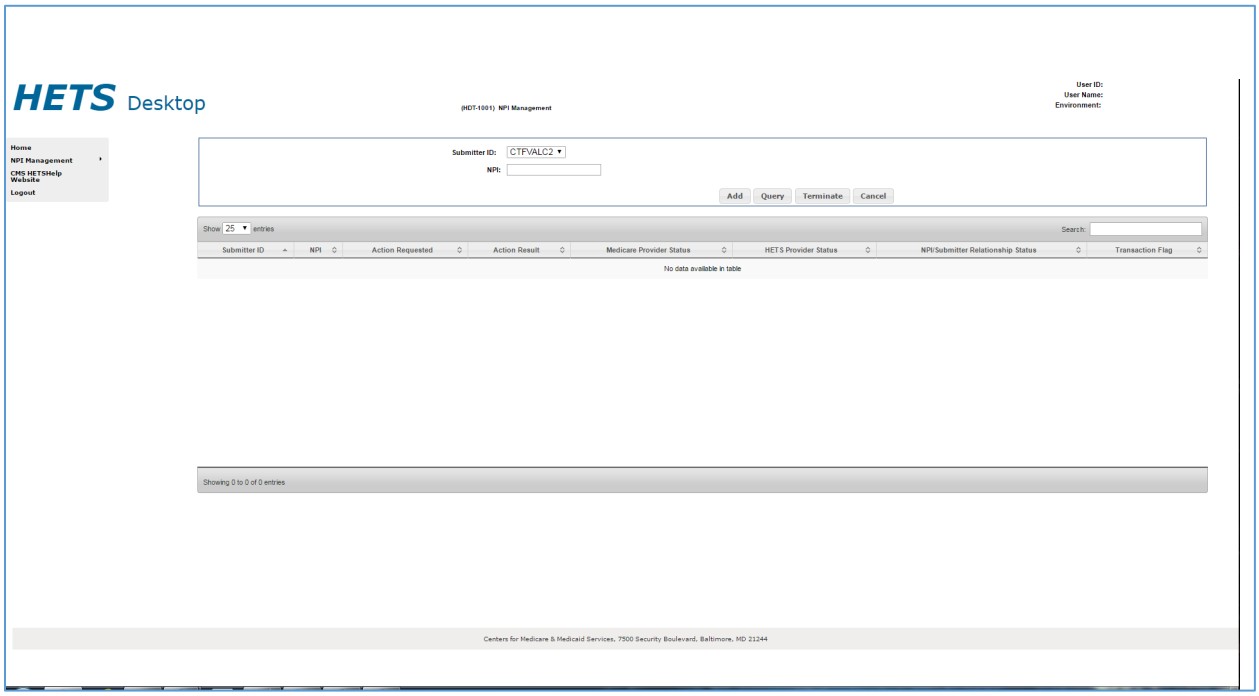
- Home – The HDT User Interface home page.
- NPI Management – Allows Submitters to add, terminate and/or query NPI numbers one at a time. This link is available to Clearinghouse and Direct Provider Submitters.
- NPI Batch Management – Provides a link to the Enterprise File Transfer (EFT) system. This 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 left-hand navigation menu. The ***HDT NPI Management Screen (HDT-1001)*** will display as illustrated in Figure 54.

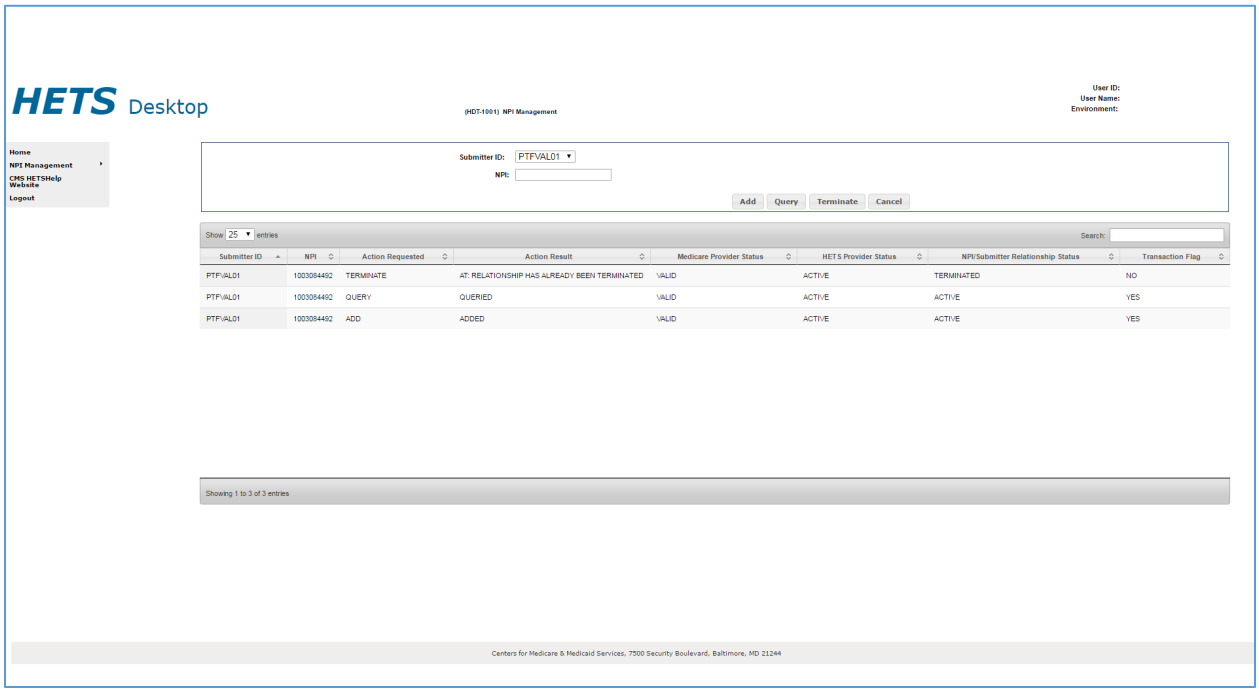
Figure 54: HDT NPI Management Screen (HDT-1001)



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.

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”.

Note: The table will display the results in the order in which the NPIs are entered into the NPI text box, with the most recent action listed first. The HDT application defaults to 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.

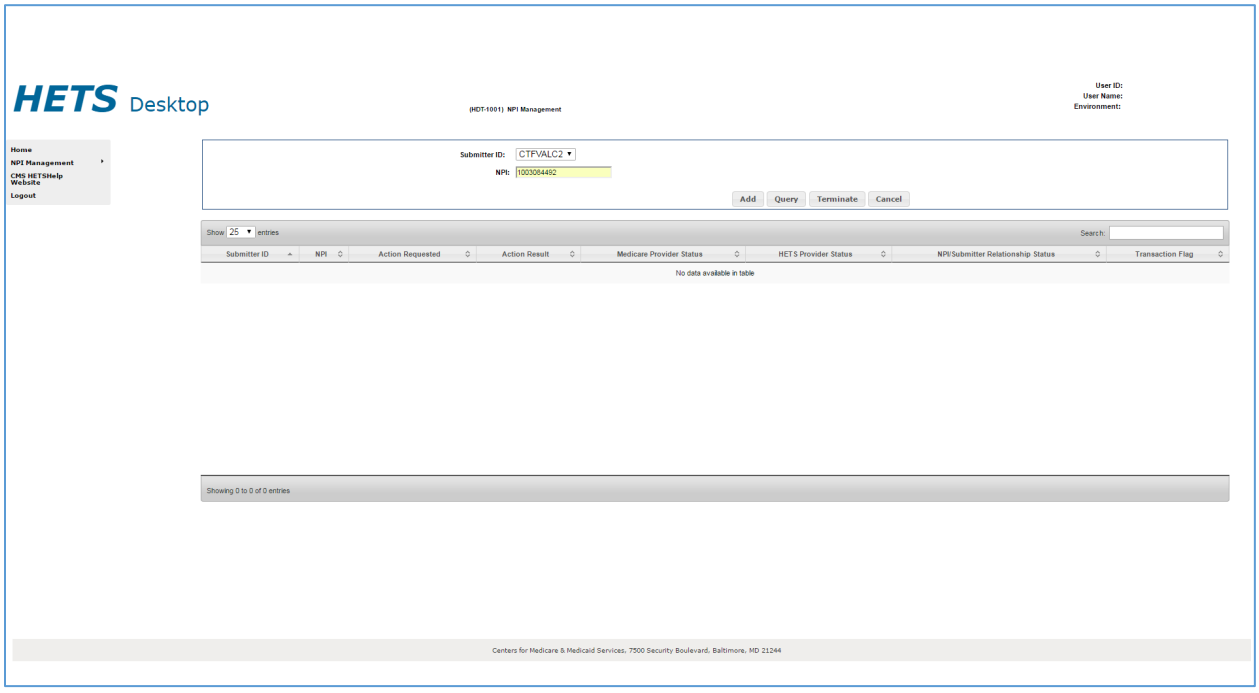
5.2.1. Query

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



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].

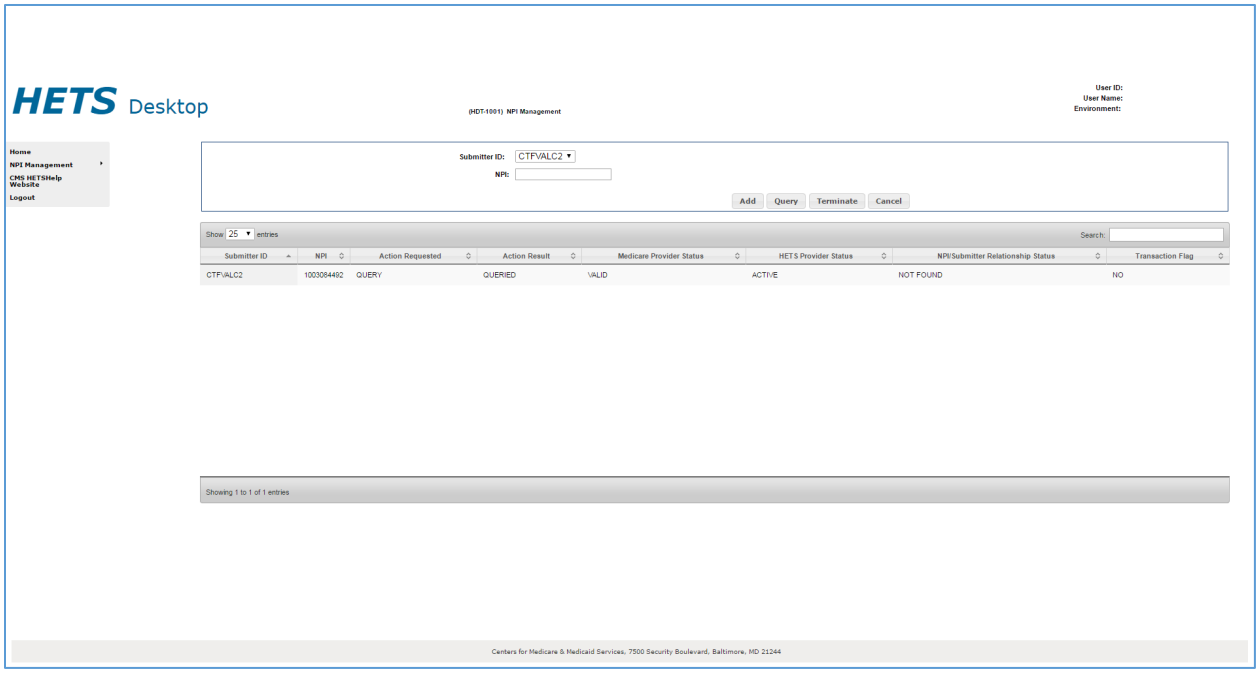
   Note: The HDT application will clear the **NPI** field when you select an NPI Management action. The Submitter ID field will not be cleared. If you wish to perform actions for a different Submitter ID associated with your

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



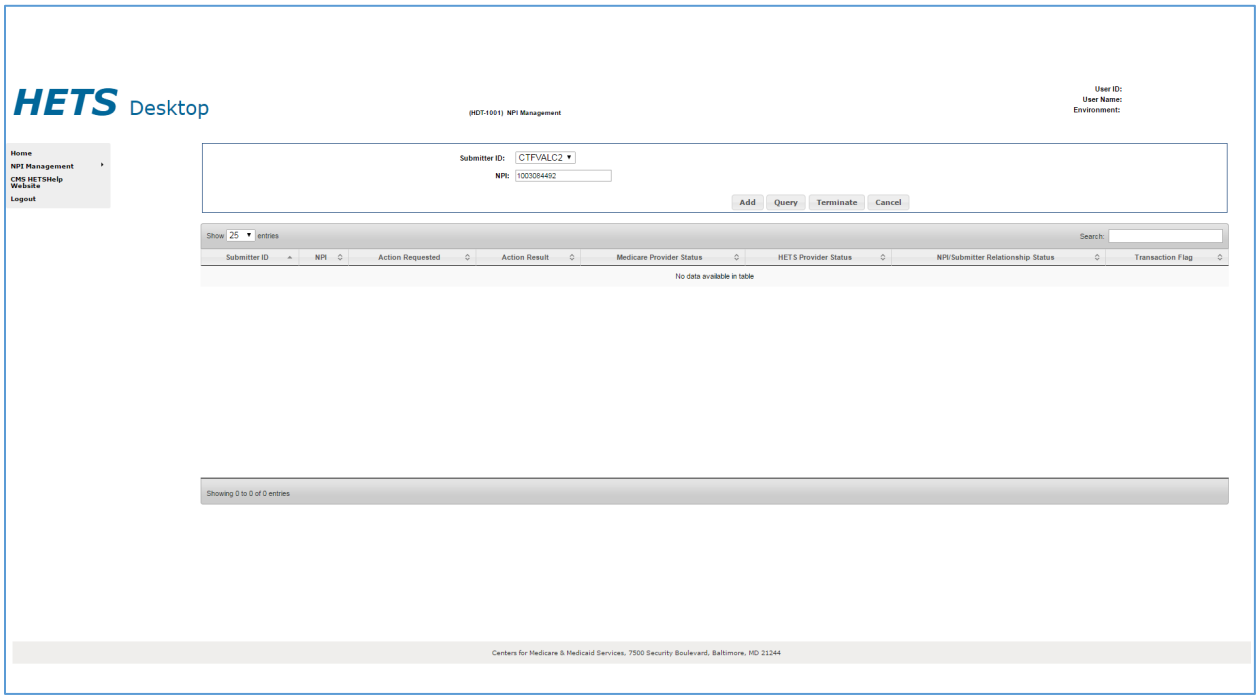
5.2.2. Add

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:

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



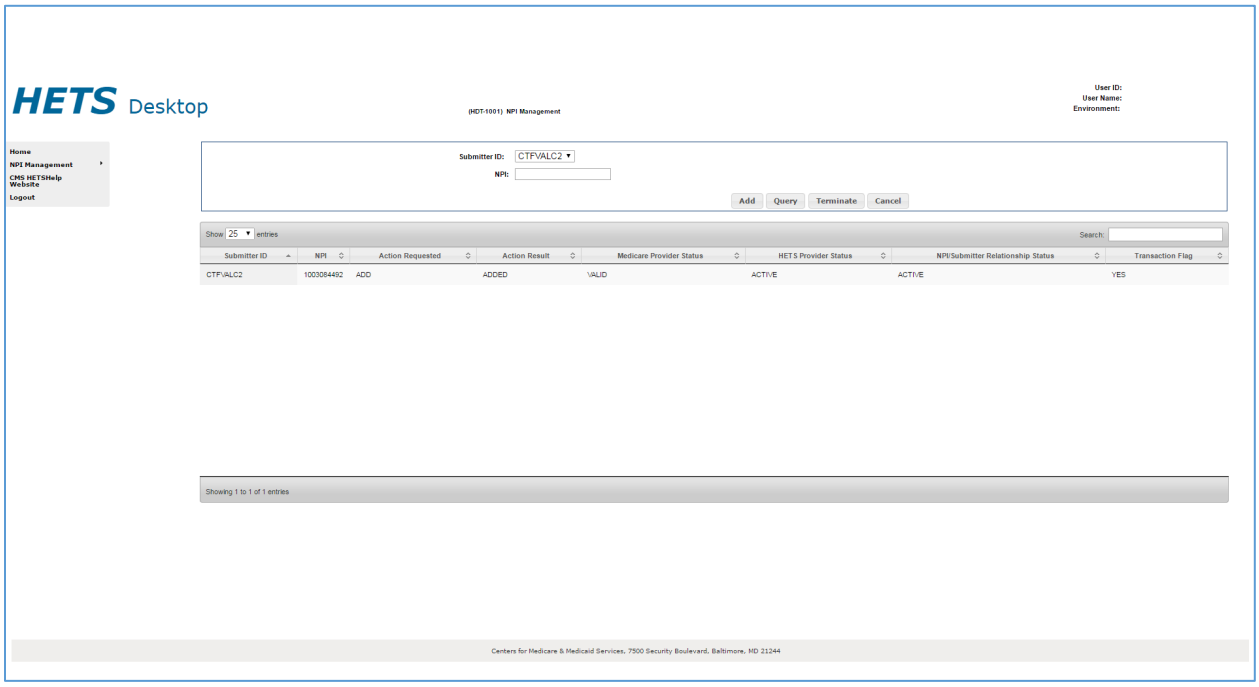
1. Select a Submitter ID from the selection box labeled Submitter ID.
2. Enter a 10-digit NPI number in the **NPI** field. HDT only accepts numeric values in the NPI field.
3. Select [Add].

   Note: 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.

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



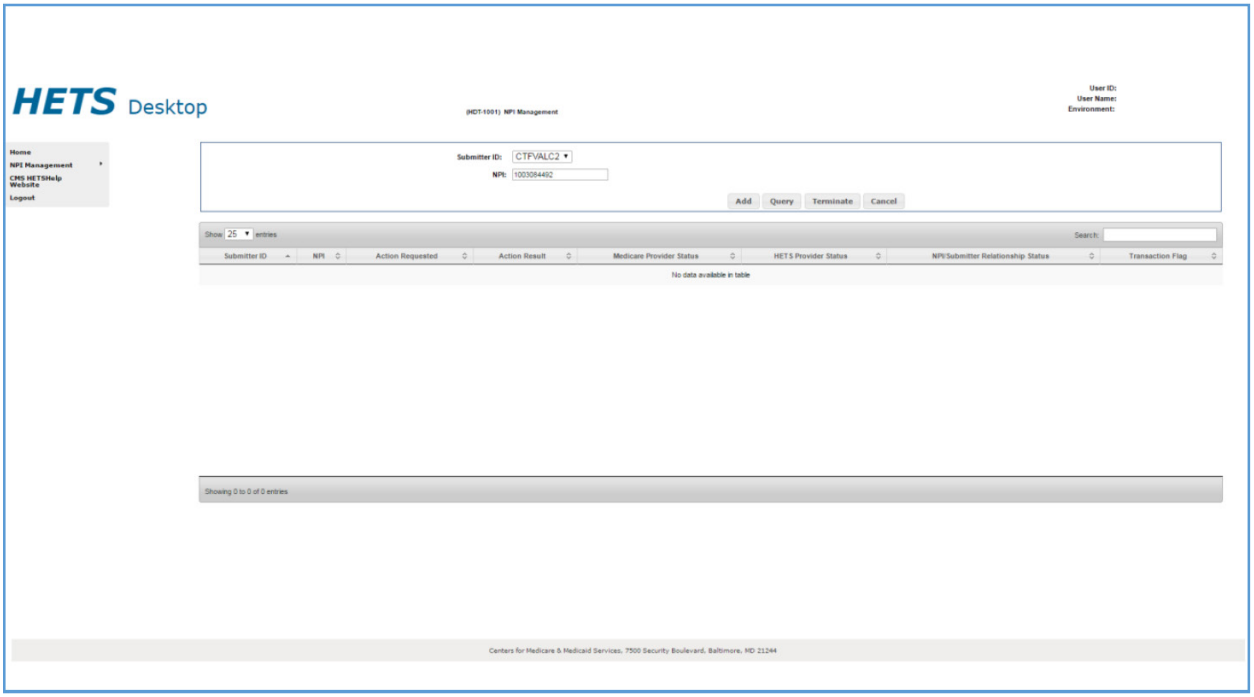
5.2.3. Terminate

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:

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



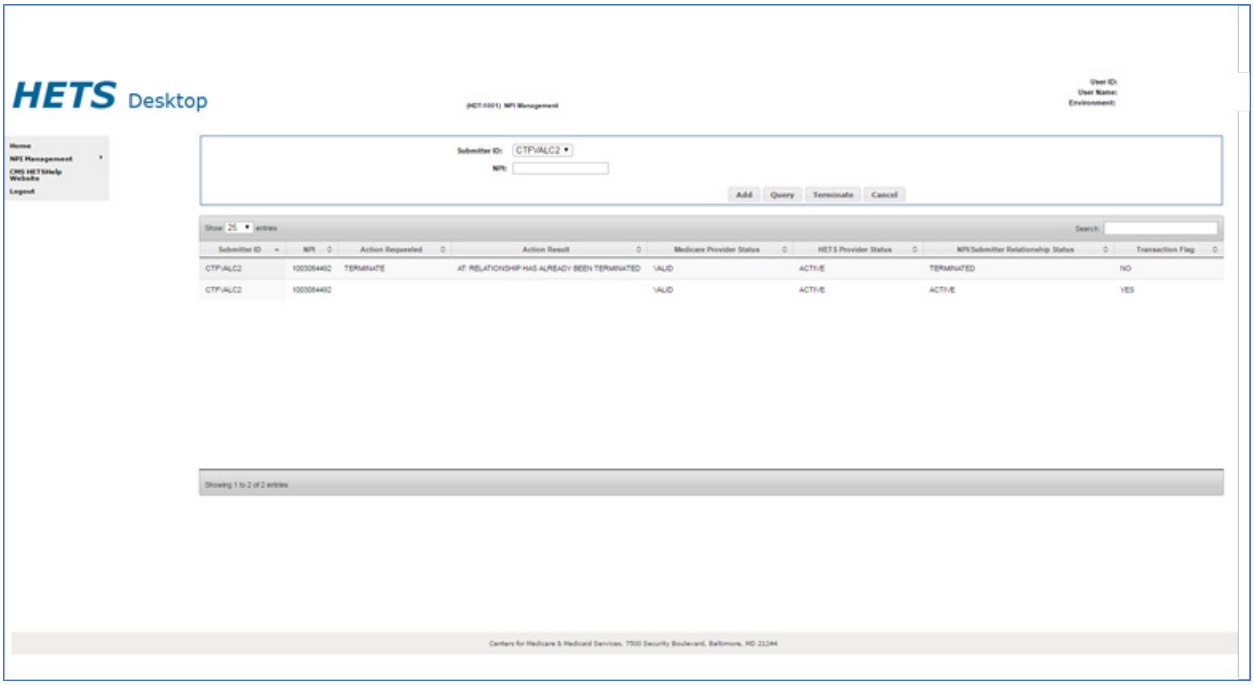
1. Select a Submitter ID from the selection box labeled Submitter ID.
2. Enter a 10-digit NPI number in the **NPI** field. HDT only accepts numeric values in the NPI field.
3. Select [Terminate].

   Note: 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.

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.

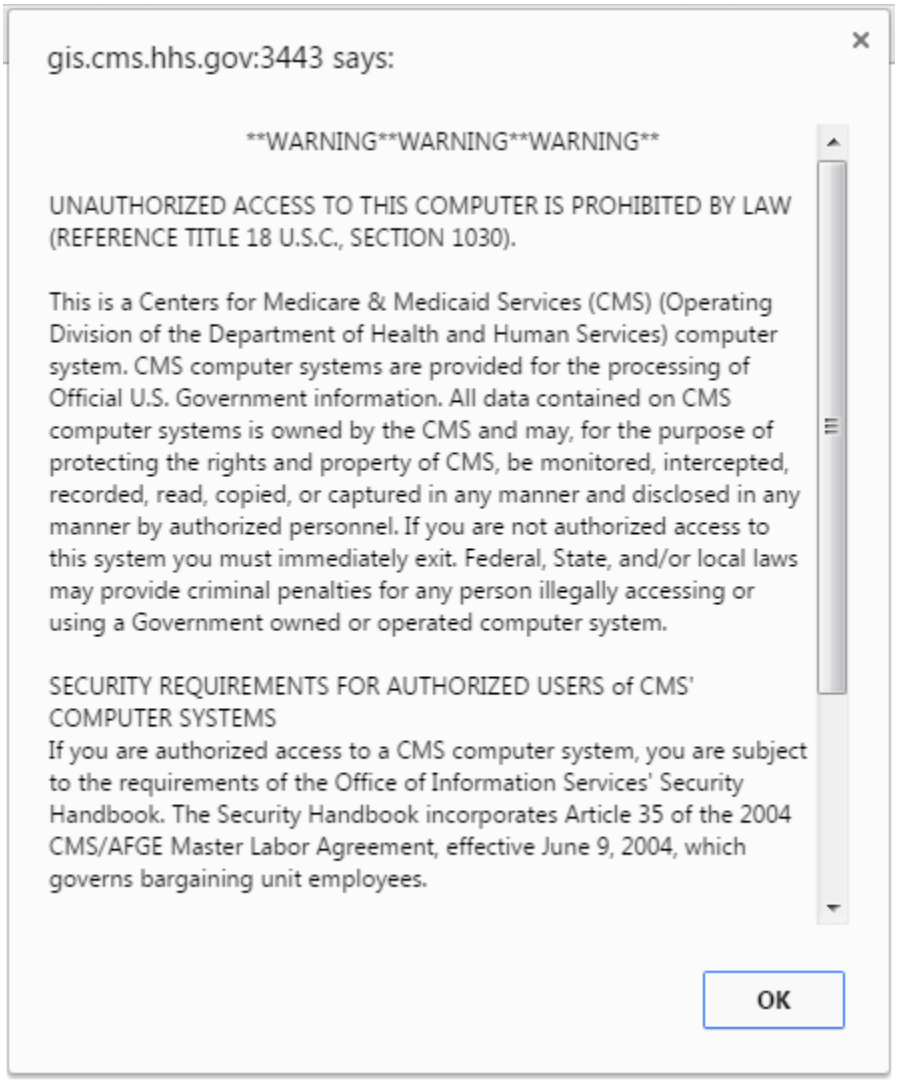
Note: Clearinghouse Submitters are limited to uploading only one batch file per day. If a Clearinghouse Submitter attempts to upload more than one file during a single calendar day, an error message is returned in the batch output file.

To access the NPI Management feature, select the [NPI Batch Management] link in the left-hand navigation menu. The ***HDT NPI Batch Management Screen (HDT-1002)*** will start the login sequence described in Section 5.3.1.

5.3.1. Login to Enterprise File Transfer (EFT)

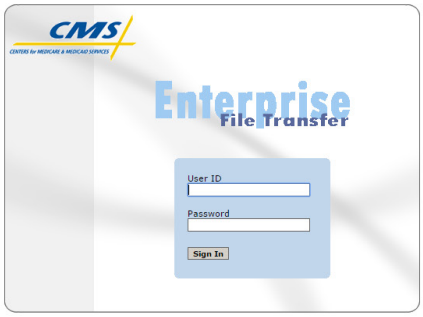
To access the NPI Batch Management feature, select the NPI Batch Management hyperlink in the left-hand navigation menu. A new window opens to display a CMS security warning, as illustrated in Figure 62. The HDT application remains open in the background. Select [OK].

Figure 62: EFT Security Warning



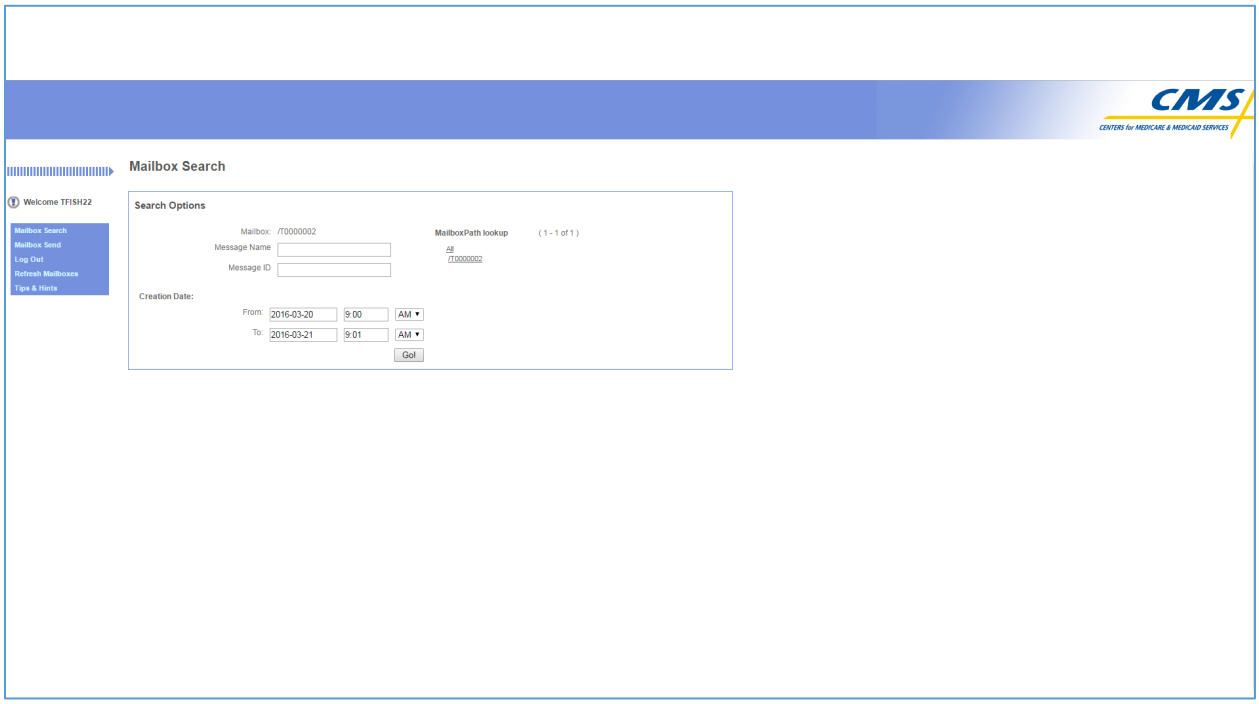
The ***Enterprise File Transfer Login*** screen now appears as illustrated in Figure 63.

Figure 63: EFT Login Screen



1. Enter your CMS Enterprise Portal User ID in the User ID field.
2. Enter your CMS Enterprise Portal password in the Password field.
3. Select [Sign In]. Once you are authenticated, the ***EFT Mailbox Search*** screen will display as illustrated by Figure 64.

Figure 64: EFT Mailbox Search Screen

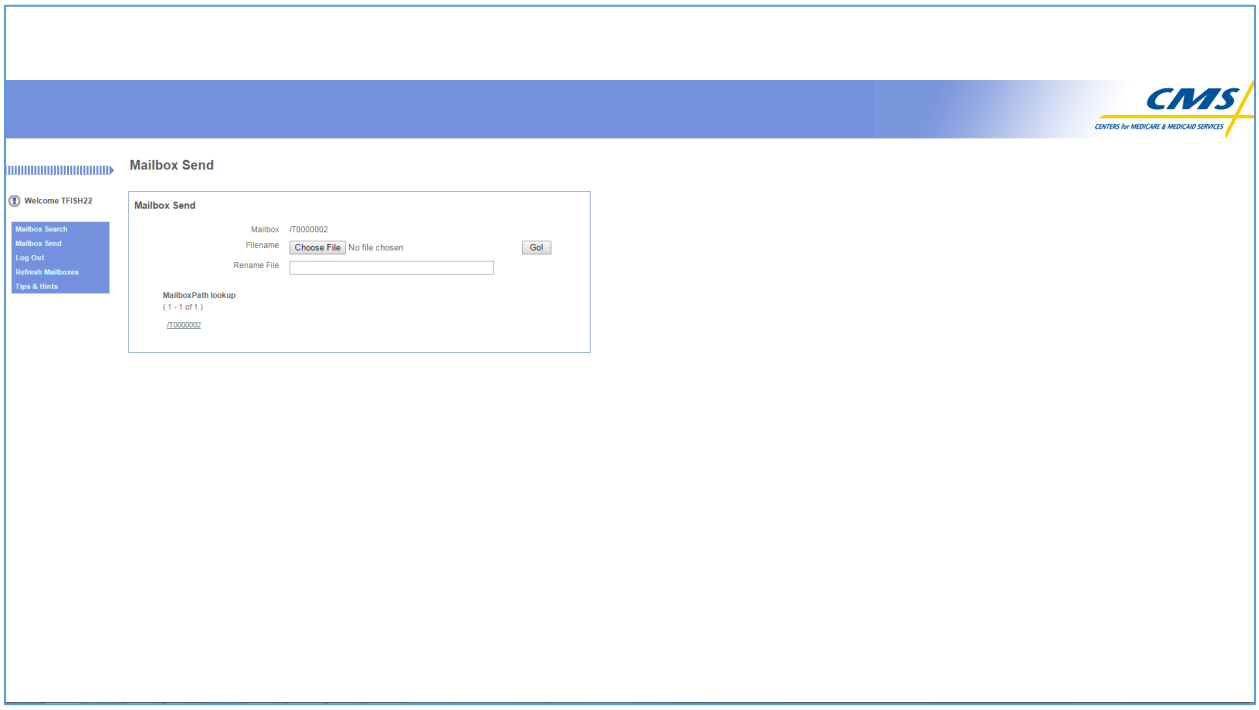


5.3.2. Uploading a File

To upload an input file, follow these steps:

1. Log into EFT following the steps in Section 5.4.1.
2. On the ***EFT Mailbox Search*** screen, illustrated in Figure 66, select the Mailbox Send hyperlink in the left hand navigation menu. The ***EFT Mailbox Send*** screen will display as illustrated by Figure 65.

Figure 65: EFT Mailbox Send Screen



3. Select [Browse].
4. Select the comma delimited, flat text file containing the multiple NPIs you wish to query, add and/or terminate.

The file naming convention is: GUID.NONE.HDT.D.Mailbox.FUTURE.P

Customizable elements:

GUID = User ID. This is the same as your CMS Enterprise Portal User ID.

Mailbox = EFT Mailbox ID. This is the Submitter ID as assigned to you by CMS. (example: C123A456)

All other file name elements are required and constant.

Note: The Mailbox field will be automatically populated with your mailbox name. You will only be able to view your own mailbox for security purposes.

5. Select [Go!]. Once the file has finished uploading, you will be redirected to the ***EFT Mailbox Search*** screen as illustrated in Figure 64.

5.3.3. Downloading a File

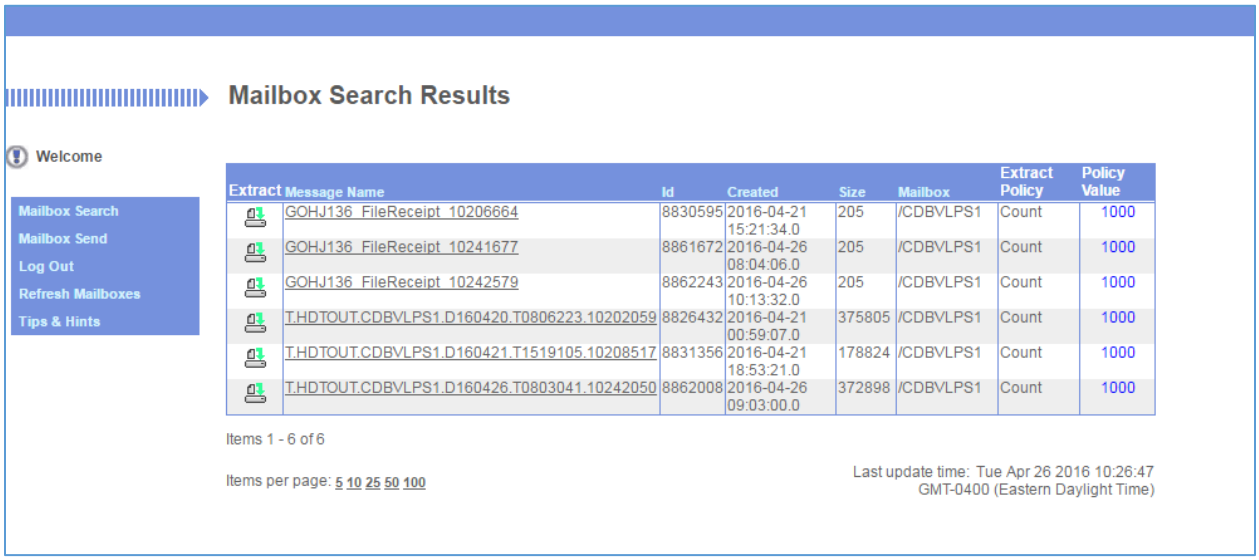
To download a results file, follow these steps:

1. Log into EFT following the steps in Section 5.4.1.
2. Select your mailbox from the Mailbox drop-down list on the ***EFT Mailbox Search*** screen, as illustrated in Figure 64. You may leave the default

Creation Date values, or you may change them to the time frame(s) you wish to search.

3. Select [Go!]. If there are any results that match your mailbox search criteria, they will display on the ***EFT Mailbox Search Results*** screen as illustrated by Figure 66.

Figure 66: EFT Mailbox Search Results Screen



The naming convention for the results file(s) is:
P.HDTOUT.Mailbox.Dyymmdd.Thhmmsst.pn

Customizable elements:

Mailbox = EFT Mailbox ID. This is the Submitter ID as assigned to you by CMS.

Dyymmdd = Date in yymmdd format

Thhmmsst – Time in hhmmsst format

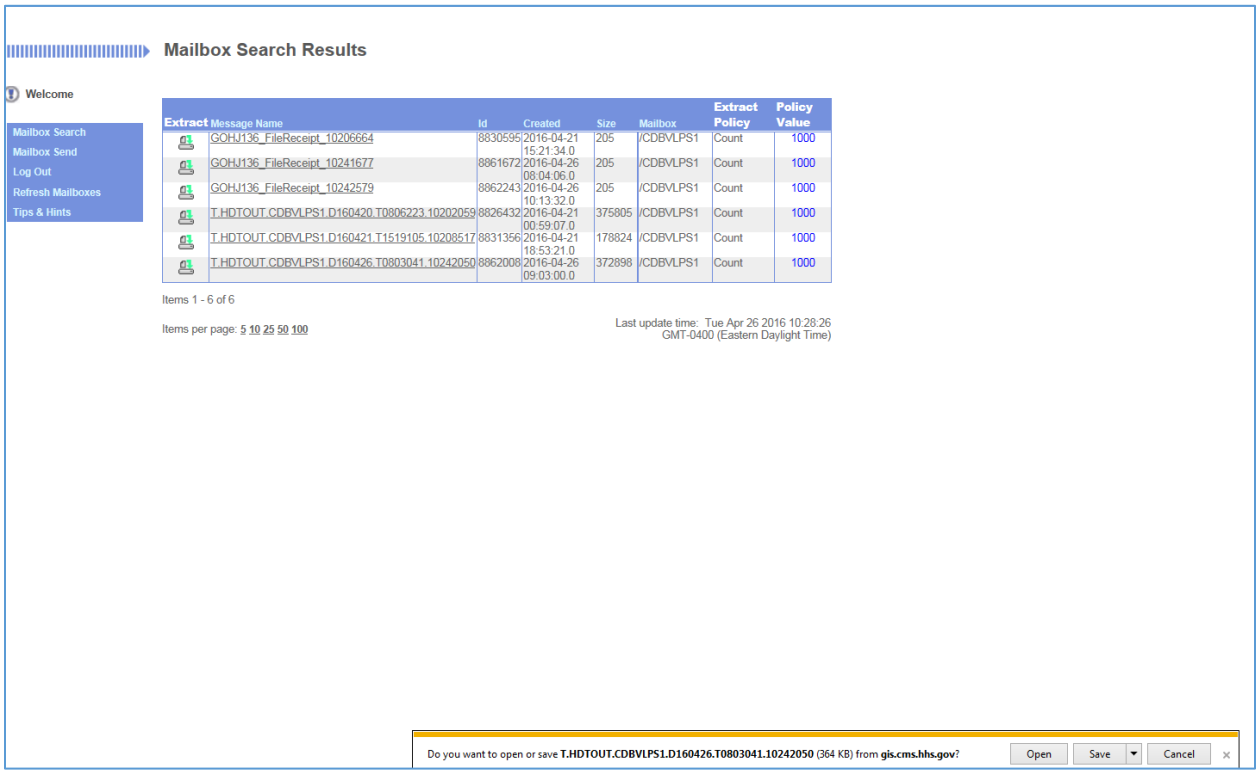
pn = Processing number assigned by EFT

All other file name elements are required and constant.

You will also receive a text file that contains confirmation that your input file was received by the file transfer system.

4. Select [Extract]. You may also select the Message Name. An ***EFT File Download*** pop-up window will display as illustrated in Figure 67.

Figure 67: EFT File Download



5. Select [Save]. The file will be saved as the default file name from the EFT mailbox. You may rename the file at your discretion once the file is saved to your computer.
6. Select [Cancel] if you decide not to save the results file.

5.4. File Formats

5.4.1. Input File

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.

Table 3: Input File Layout and Element Description

Data Element	Data Type	Length	Possible Values	Description
Submitter ID	Alphanumeric	8		The 8-character Submitter ID associated with the Clearinghouse.

Data Element	Data Type	Length	Possible Values	Description
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.

Sample Input File

File Name: ZYXW123.NONE.HDT.D.C123A456.FUTURE.P
C123A456,1111111111,Q
C123A456,2222222222,Q
C123A456,3333333333,A
C123A456,3333333333,A
C123A456,4444444444,A
C123A456,5555555555,A
C123A456,6666666666,T
C123A456,6666666666,T
C123A456,7777777777,T

5.4.2. Output File

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.

Table 4: Output File Layout

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.

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: P.HDTOUT.C123A456.D100101.T0122331.9876543
File processed on 01/01/2010 01:22
C123A456,1111111111,Q,Q,A,V,A,A,Y
C123A456,2222222222,Q,Q,A,I,T,T,N

C123A456,3333333333,A,A,A,V,A,A,Y
C123A456,3333333333,A,AE,A,V,A,A,Y
C123A456,4444444444,A,SP,A,V,S,S,N
C123A456,5555555555,A,IM,A,I,NF,NF,N
C123A456,6666666666,T,T,A,V,A,T,N
C123A456,6666666666,T,AT,A,V,A,T,N
C123A456,7777777777,T,NE,A,I,NF,NF,N

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

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 Section 6.5.

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.

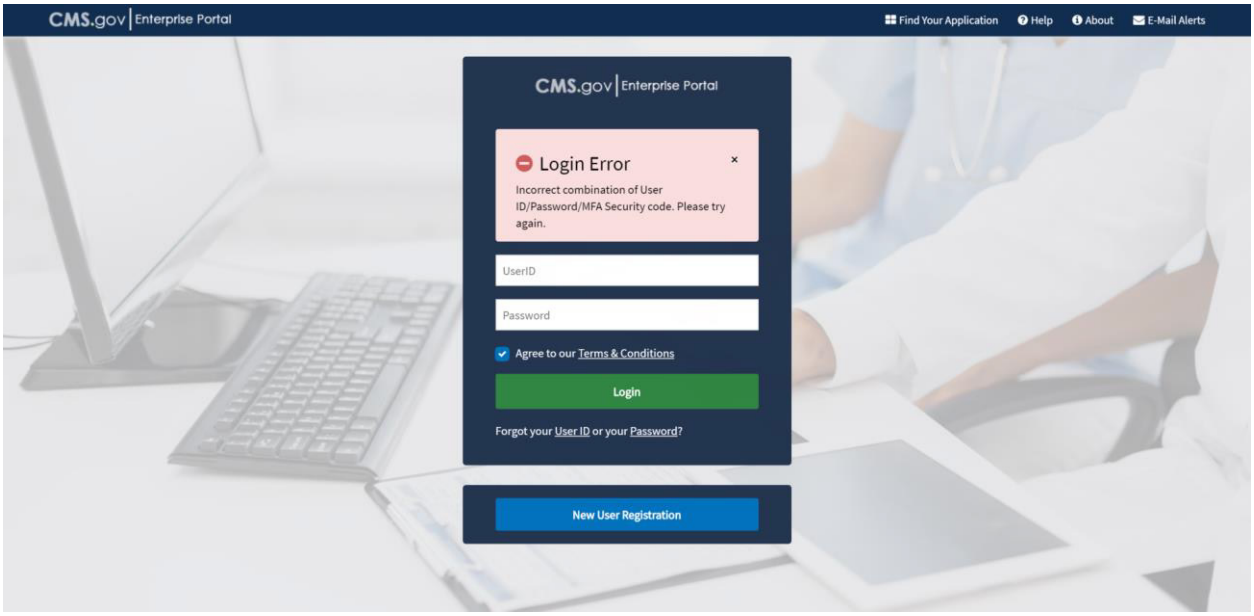
Table 5: Access and Behavior Error Messages

Error Message
Message 100
Message 110
Message 120
Message 130
Message 700
Message 710
Message 720
Message 730
Message 740
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.

Figure 68: Incorrect ID, Password or Security Code Screen



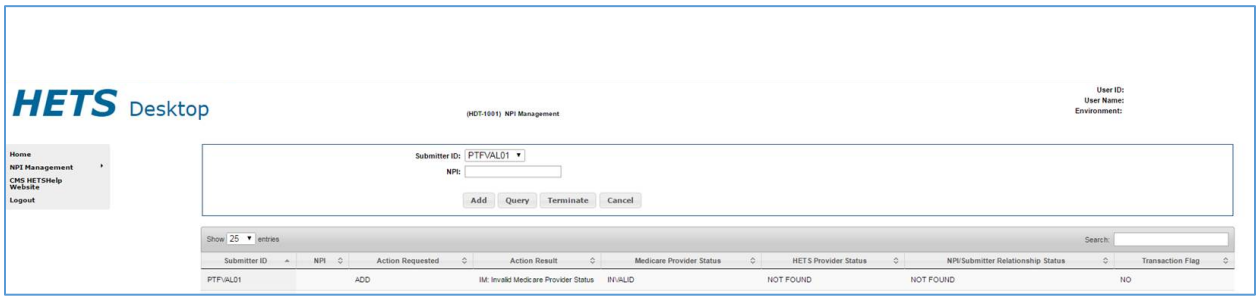
Enter a valid CMS Enterprise Portal User ID in the **User ID** field. Select [Next].

If you have forgotten your CMS Enterprise Portal User ID or password, refer to Section 4.3.3 for more information. If you continue to encounter issues logging into the CMS Enterprise Portal, please refer to Section 6.5 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



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 invalid. File could not be processed further.	The Submitter ID within the file is: Not found, Not associated with the Submitter ID in the file name, Suspended, or Terminated.
A file has already been submitted by Submitter ID ${Submitter ID}. A Submitter can only submit one file in a day.	A Submitter uploads more than one file during a single calendar day using the NPI Batch Management function in HDT.

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 MCARE@cms.hhs.gov Monday through Friday, from 7:00 AM to 7:00 PM ET.

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

7. GLOSSARY

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.

Table 7: Acronyms and Definitions

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