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

Health Insurance Portability and Accountability Act (HIPAA) Eligibility Transaction System (HETS) Provider Graphical User Interface (GUI) (HPG)

User Guide

Final

Version: 2-1

Effective Date: June 2016

REVISION HISTORY

Table 1: Document Revision History

Version	Date	Description of Changes
1.0	06/22/2010	Baseline Version
1.1	07/23/2010	Changes include: Updated screenshots for HPG CMS Warning Page and HPG Home Page. Added Help Page screenshot to section 6.5. Updated CMS applications portal URLs.
1.2	08/13/2010	Changes include: Section 2 – Removed reference to the IACS guide and replaced it with information on how to contact the MCARE Helpdesk Section 4.3.1 – added section on how to request access to HPG if a Submitter already has an IACS account. Section 4.3.1 – Removed reference to the IACS guide and replaced it with information on how to contact the MCARE Helpdesk Section 5.4 – added note regarding one file per submitter per day. Section 5.5.1 – Table 3 updated with field length column. Section 6.1 – updated with HPG availability and added explanation on what happens if a file is processing when the database becomes unavailable. Section 6.3.5 – Table 5 updated with error messages. Section 6.4.2 – added section to emphasize one file per submitter per day.

Version	Date	Description of Changes
1.3	11/08/2011	Changes Include: Replaced all instances of Gentran with Sterling. Section 4.3.2 – IACS New User Registration: Figure 6: User Information Section of New User Registration Screen Add the following new figures: Figure 7: Access Request Section of New User Registration Screen Figure 8: Professional Contact Information Screen Figure 9: Authentication Questions Screen Section 5.4.1 – The following figures have been updated to reflect the new Sterling system: Figure 19: Sterling Login Screen Figure 20: Sterling Mailbox Search Screen Figure 21: Sterling Mailbox Send Screen Figure 22: Sterling Mailbox Search Results Screen Figure 23: Sterling File Download
1-4	12/20/2011	Changes include: Sections 2, 4.3.1, 6.1 and 6.55 – Updated MCARE hours of operation.
1-5	02/11/2014	Changes include: Updated the IACS Terms and Conditions screenshot as well as the Login screenshot in relation to EIDM backend updates.

Version	Date	Description of Changes
1-6	02/05/2015	Changes include: Section 2 – Updated HETS Companion Guide URL. Added introduction and link to EIDM User Guide. Section 3 – Added paragraph to explain that HPG is accessed following EIDM authentication. Section 4 – Complete revision to modify authentication processes from IACS to EIDM. Added note indicating that HPG only allows EIDM User IDs of 32 characters or less. Sections 5 & 7 – Updated Figure numbers and references to reflect changes made to the overall document. Section 8 – Table 6 updated with EIDM definition; IACS removed from table.
1-7	08/07/2015	Changes include: Updated references from EIDM system and User IDs to CMS Enterprise Portal system and User IDs. Section 4 – Added notes indicating that HETS HPG application does not allow special characters to be used in the CMS Enterprise Portal User ID and/or password. Replaced all references from Sterling to EFT. Updated Figures 19-24 to reflect EFT system design. Minor formatting changes throughout the document.
1-8	08/27/2015	Changes include: Section 4.3.5 – Updated section to direct the user to log into HPG through the CMS Enterprise Portal. Replaced Figures 1-3 with a new Figure 1 to reflect the change in HPG login location through the CMS Enterprise Portal.

Version	Date	Description of Changes
1-9	12/03/2015	Changes include: Section 2 – Added URL for HETS HPG RIDP / MFA FAQs document. Section 4.1 – Updated the Set-up Considerations based on current CMS technical recommendations, including that Users should avoid using browser bookmarks. Section 4.3.1 – Updated document to include step-by-step instructions regarding adding the HPG role to an existing CMS Enterprise Portal account, including RIDP. Section 4.3.2 – Updated document to include step-by-step instructions regarding creating a CMS Enterprise Portal User account. Section 4.3.4 – Added Section 4.3.4 detailing CMS Enterprise Portal Multi-Factor Authentication (MFA) requirements and processes. Section 4.3.5 – Added Section 4.3.5 detailing CMS Enterprise Portal Remote Identity Proofing (RIDP) requirements and processes. Table 6 – Added MFA & RIDP to the list of acronyms.
2-0	4/08/2016	Changes include: Section 4.3.4.2 – Added a statement that CMS discourages Users from utilizing Autofill features of internet browsers. Section 4.3.4.3 – Added new section outlining a new option for registered Users to receive an MFA Security Code when they are not in possession of their registered MFA Device. Section 4.3.6 – Updated screen shots and modified the process to reflect that the CMS Enterprise Portal now only requires a single MFA login for HPG Users.

Version	Date	Description of Changes
2-1	06/27/2016	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 6.3.5 – Removed the last row from Table 5, 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.

TABLE OF CONTENTS

User Guide 1
Final 1
REVISION HISTORY ii
TABLE OF CONTENTS vii
LIST OF FIGURES viii
LIST OF TABLES x
1. INTRODUCTION 1
2. REFERENCED DOCUMENTS 1
3. APPLICATION OVERVIEW 2
3.1. Conventions 3
3.2. Cautions and Warnings 3
4. GETTING STARTED 3
4.1. Set-up Considerations 3
4.2. User Access Considerations 4
4.3. Accessing the HPG Application 4
4.3.1. Requesting HPG Access for an Existing CMS Enterprise Portal Account 4
4.3.2. CMS Enterprise Portal New User Registration 18
4.3.3. CMS Enterprise Portal User ID and Password Management 24
4.3.4. Multi-Factor Authentication (MFA) 25
4.3.5. Remote Identity Proofing (RIDP) 41
4.3.6. Login to the HPG Application 42
4.4. Application Organization & Navigation 46
4.5. Exiting the Application 46
5. USING THE APPLICATION 47
5.1. Application Layout 47
5.2. Submitter Profile 49
5.3. NPI Management 49
5.3.1. Query 52
5.3.2. Add 53
5.3.3. Terminate 54
5.4. NPI Batch Management 55
5.4.1. Login to Enterprise File Transfer (EFT) 55
5.4.2. Uploading a File 57
5.4.3. Downloading a File 58
5.5. File Formats 60
5.5.1. Input File 60
5.5.2. Output File 61
6. TROUBLESHOOTING & SUPPORT 66
6.1. Troubleshooting 66
6.2. Connectivity 66
6.3. Error Messages 67
6.3.1. Unauthorized Access 67
6.3.2. CMS Enterprise Portal Login 67
6.3.3. Invalid Submitter ID 68
6.3.4. Missing or Invalid NPI 68

6.3.5. Batch File Error Messages 68
6.4. Special Considerations 69
6.4.1. Data Size Limits 69
6.4.2. Daily Batch File Submission 69
6.5. System Support Information 69
7. GLOSSARY 70
8. ACRONYMS 70

LIST OF FIGURES

Figure 1: CMS Enterprise Portal Screen 5
Figure 2: Login to CMS Secure Portal 5
Figure 3: Terms and Conditions Screen 6
Figure 4: Login to CMS Enterprise Portal 6
Figure 5: Enter Security Code 7
Figure 6: My Access Screen 8
Figure 7: My Access Screen 9
Figure 8: Request Access 9
Figure 9: Select a Role 10
Figure 10: HPG User Role Identity Verification 10
Figure 11: Identity Verification Screen 11
Figure 12: Terms and Conditions Screen 12
Figure 13: Your Information Screen 13
Figure 14: Verify Identity 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 16
Figure 18: Request New Application Access Review 17
Figure 19: Request New Application Access Acknowledgement 18
Figure 20: CMS Enterprise Portal Screen 18
Figure 21: New User Registration 19
Figure 22: Terms and Conditions Screen 20
Figure 23: Your Information Screen 21
Figure 24: Choose User ID and Password 22
Figure 25: Create and Confirm Password 22
Figure 26: Select Challenge Questions and Answers 23
Figure 27: Registration Complete 24
Figure 28: CMS Enterprise Portal Screen 25
Figure 29: Login to CMS Secure Portal 26
Figure 30: Terms and Conditions Screen 26
Figure 31: Login to CMS Enterprise Portal 27
Figure 32: Enter Password Screen 27
Figure 33: Select My Profile 28
Figure 34: Register Phone, Computer, or Email 29
Figure 35: Select Credential Type 30
Figure 36: Symantec Credential ID 30
Figure 37: Select Phone/Tablet/PC/Laptop as Credential Option 31

Figure 38: Select Email as Credential Option..... 32
Figure 39: Select Text as Credential Option..... 33
Figure 40: Select IVR as Credential Option..... 34
Figure 41: Complete New Application Access..... 35
Figure 42: Unable to Access Security Code Begin Navigation..... 35
Figure 43: Unable to Access Security Code User ID Entry 36
Figure 44: Unable to Access Security Code Challenge Questions..... 36
Figure 45: Unable to Access Security Code Challenge Completion..... 37
Figure 46: CMS Enterprise Portal Screen 37
Figure 47: Login to CMS Secure Portal..... 38
Figure 48: Terms and Conditions Screen..... 38
Figure 49: Enter CMS Enterprise Portal User ID..... 39
Figure 50: Enter Security Code 39
Figure 51: Select My Profile 40
Figure 52: Remove Your Phone or Computer 41
Figure 53: Removal of Registered MFA Device Complete 41
Figure 54: CMS Enterprise Portal Terms and Conditions Screen 43
Figure 55: Welcome to the CMS Enterprise Portal Login Screen – Access to HPG 44
Figure 56: Enter Security Code 44
Figure 57: HPG User Interface Warning Screen 45
Figure 58: HPG User Interface Home Screen 46
Figure 59: CMS Enterprise Portal Web Access Management (Logout) Screen 47
Figure 60: HPG Application Site Map..... 48
Figure 61: HPG User Interface Home Screen 48
Figure 62: HPG User Interface Submitter Profile Screen 49
Figure 63: HPG User Interface NPI Management Screen..... 50
Figure 64: HPG User Interface NPI Management Screen – Results..... 50
Figure 65: HPG User Interface NPI Management Screen – Query 52
Figure 66: HPG User Interface NPI Management Screen – Query Results 53
Figure 67: HPG User Interface NPI Management Screen – Add 53
Figure 68: HPG User Interface NPI Management Screen – Add Results..... 54
Figure 69: HPG User Interface NPI Management Screen – Terminate..... 54
Figure 70: HPG User Interface NPI Management Screen – Terminate Results..... 55
Figure 71: EFT Security Warning 56
Figure 72: EFT Login Screen 56
Figure 73: EFT Mailbox Search Screen 57
Figure 74: EFT Mailbox Send Screen 58
Figure 75: EFT Mailbox Search Results Screen 59
Figure 76: EFT File Download..... 60
Figure 77: Unauthorized Access Screen 67
Figure 78: Incorrect ID or Password Screen 67
Figure 79: Invalid Submitter ID Screen..... 68
Figure 80: NPI Management – Invalid NPI Screen..... 68
Figure 81: Help Desk Support Screen..... 70

LIST OF TABLES

Table 1: Document Revision History ii
Table 2: Typographical Conventions 3
Table 3: Input File Layout and Element Description 60
Table 4: Output File Layout 62
Table 5: Batch File Error Messages 69
Table 6: Acronyms and Definitions 71

1. INTRODUCTION

This user guide provides the information necessary for Clearinghouse and Direct Provider Submitters to effectively use the HIPAA Eligibility Transaction System (HETS) Provider Graphical User Interface (HPG) 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 HPG 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 web site 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 this document, referred to as the CMS Enterprise Portal. The complete EIDM/CMS Enterprise Portal User Guide may be accessed via this web site link:

http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/IACS/Downloads/IACS-EIDM-Migration-User-Guide.pdf

CMS has published a list of Frequently Asked Questions (FAQs) regarding the Remote Identity Proofing (RIDP) and Multi-Factor Authentication (MFA) processes used for HETS. These FAQs may be accessed via this web site link:

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

If problems and/or questions arise while accessing the HPG 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 HPG application after authenticating their identity using a CMS Enterprise Portal User ID and password. Approved CMS Enterprise Portal Users must add the HPG role to their CMS Enterprise Portal profile from the CMS Portal Access Catalog then obtain CMS approval before HPG access will be granted.

The HPG 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 HPG application,
- Review their current Submitter profile.

The HPG 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, HPG 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 HPG 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 HPG 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 HPG 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 HPG 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 HPG 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

HPG. 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 HPG 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 HPG application sessions. Users should follow the instructions provided in this document.

4. GETTING STARTED

This section explains the HPG 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

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

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

HPG 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 HPG application. CMS also discourages Users from utilizing Autofill features of internet browsers.

4.2. User Access Considerations

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

HPG Users must have a CMS Enterprise Portal User ID that is 32 characters or less to utilize the HPG application. The HPG application also requires that CMS Enterprise Portal User IDs and passwords contain alphanumeric characters only. Special characters such as @ and – are not compatible with HPG. CMS Enterprise Portal Users who request the HPG 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 HPG application. CMS Enterprise Portal Users that utilize HPG should also ensure that their CMS Enterprise Portal password does not contain any special characters.

4.3. Accessing the HPG Application

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

4.3.1. Requesting HPG 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 HPG role to your existing profile.

Note: CMS Enterprise Portal Users that add the HPG 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.

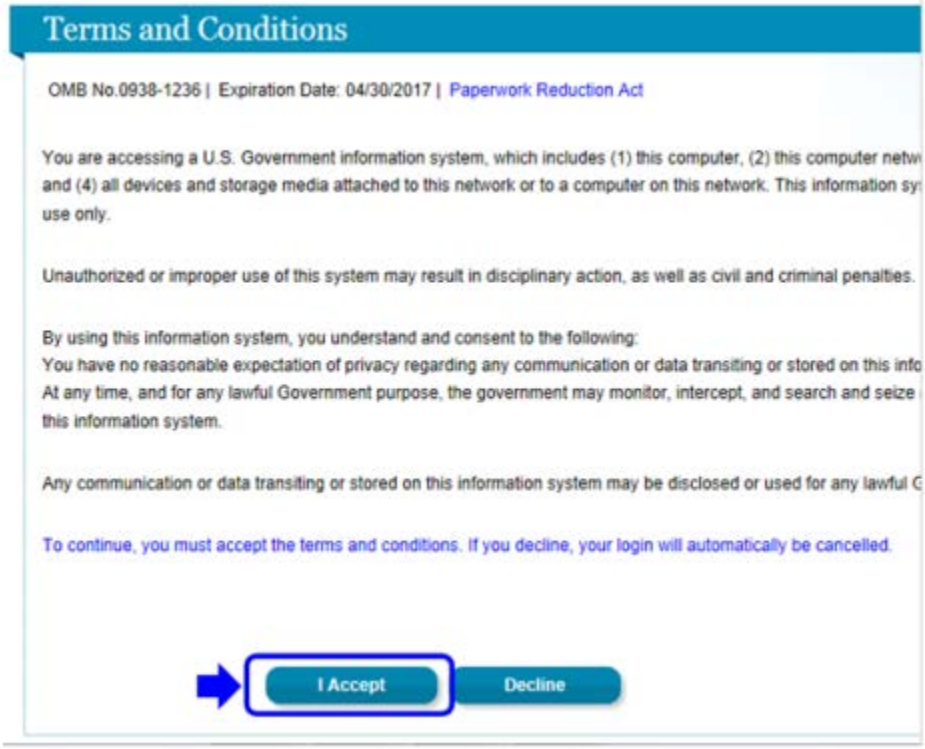
Figure 1: CMS Enterprise Portal Screen

2. Select [Login to CMS Secure Portal], as illustrated in Figure 2.

Figure 2: Login to CMS Secure Portal

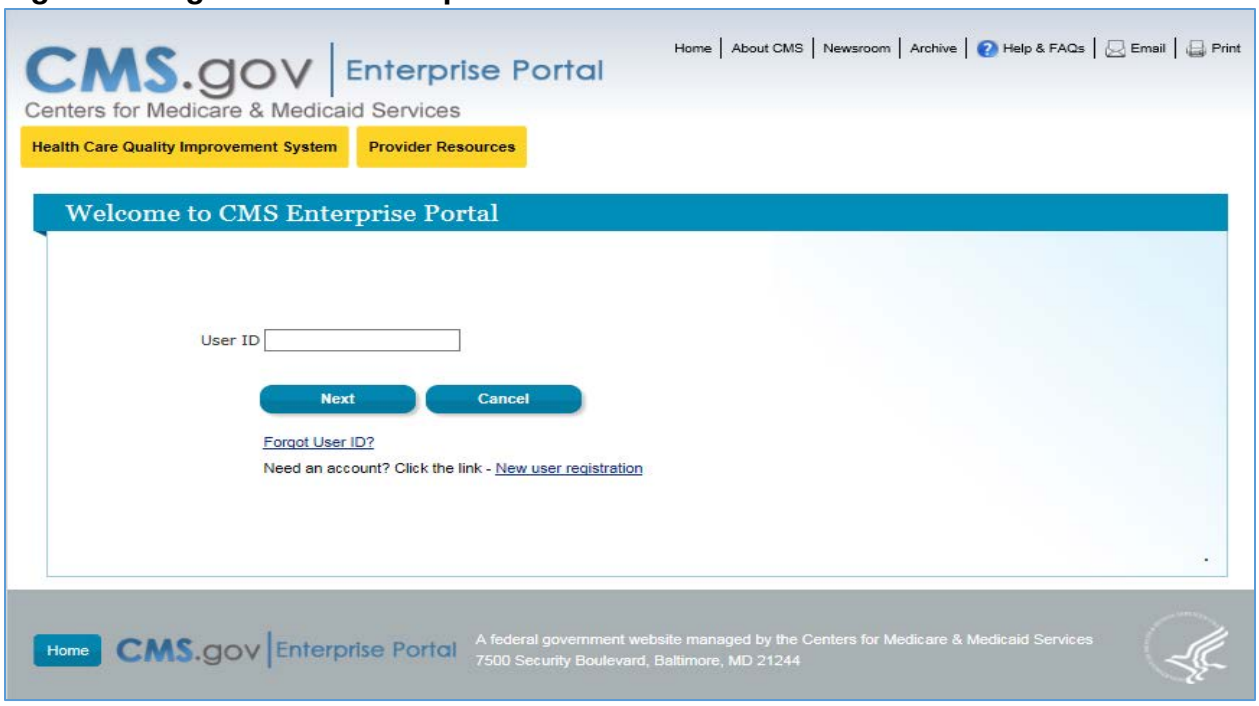
3. Read the Terms and Conditions. Select [I Accept] if you agree with the information on the screen, as illustrated in Figure 3. Select [Decline] if you don't want to proceed any further or if you want to exit the application.

Figure 3: Terms and Conditions Screen



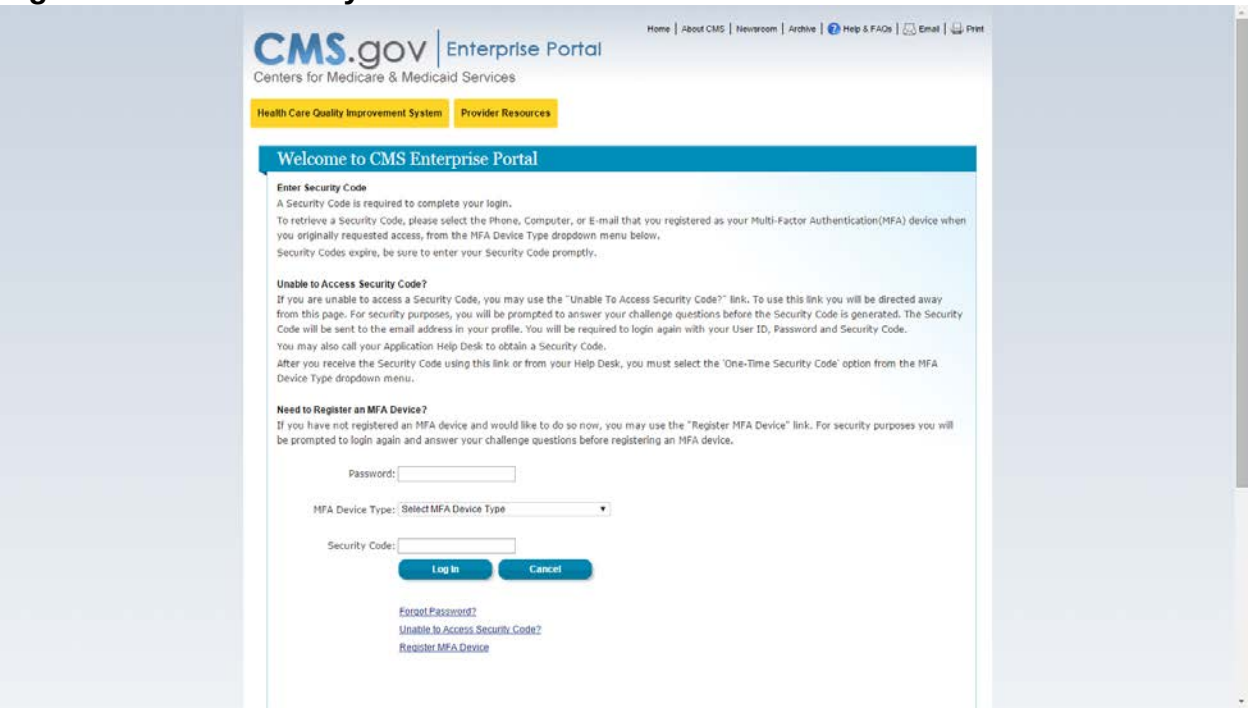
4. If you select [I Accept], the ***Welcome to CMS Enterprise Portal login*** screen will display as illustrated in Figure 4 that allows authorized Users to access the HDT application.

Figure 4: Login to CMS Enterprise Portal



5. Enter your CMS Enterprise Portal User ID in the **User ID** field.
6. Select [Next]. The ***Enter Security Code Screen*** will display as illustrated in Figure 5.

Figure 5: Enter Security Code



7. Enter your CMS Enterprise Portal password in the **Password** field.
8. 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. 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]. If the Users account has not already escalate 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, then [Log In].

   Notes:

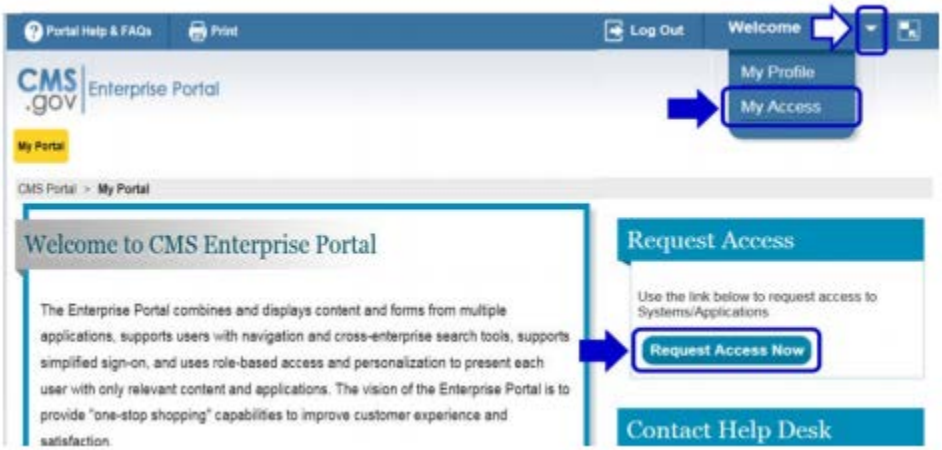
   - If you need to register a MFA Device, select the [Register MFA Device] link and complete the process described in Section 4.3.4.1.
   - If you have registered a MFA Device but are temporarily unable to access that device, you may utilize the [Unable to Access Security Code] link. See Section 4.3.4.2 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.

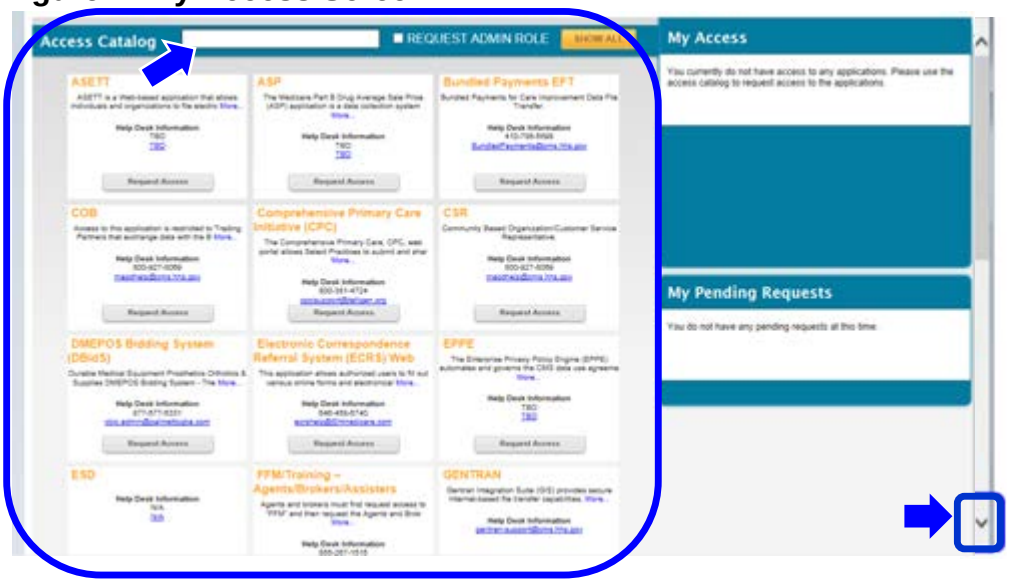
9. After logging in, the ***Welcome to CMS Enterprise Portal*** page is displayed, as illustrated in Figure 6. Select the [down arrow icon] that appears next to your name at the top of page. Then, select [My Access] from the drop down menu to continue. Alternately, you may select [Request Access Now] to continue.

Figure 6: My Access Screen



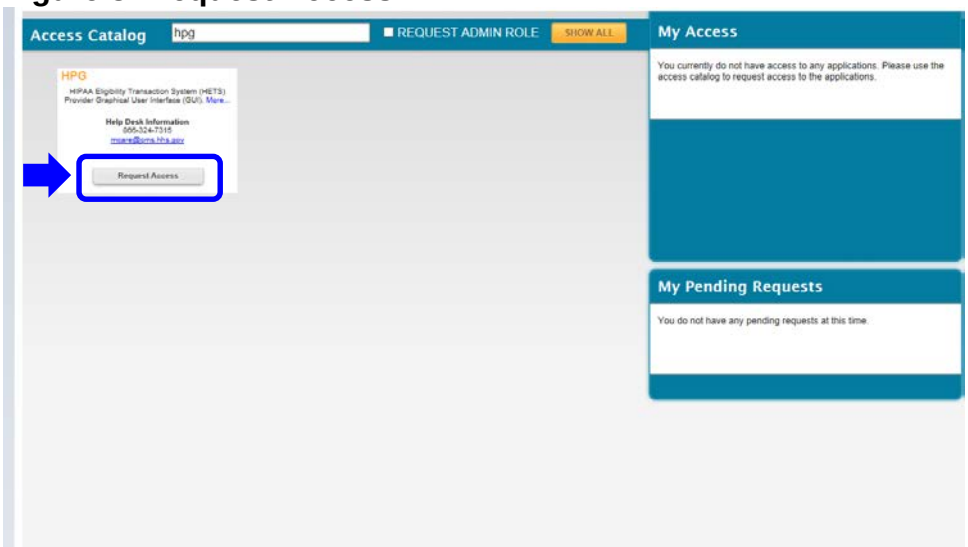
10. The [Access Catalog], [My Access] and [My Pending Requests] sections are displayed, as illustrated in Figure 7. Scroll down to locate the application you need, if it is not displayed. Alternatively, enter the first few letters of the application in the [Search] section and all of the applications 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 7: My Access Screen



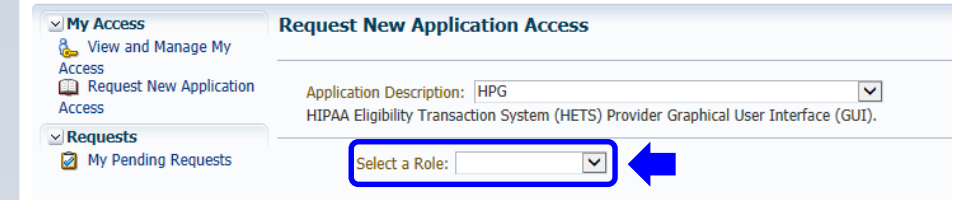
11. After entering the first few letters of the application in [Search], the applications beginning with those letters are displayed, as illustrated in Figure 8. Select [Request Access] for the HETS Provider GUI (HPG) application.

Figure 8: Request Access



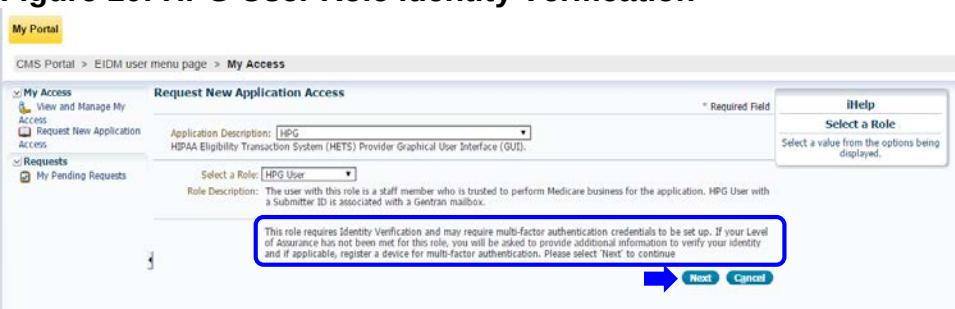
12. The Application Description and Select a role sections are displayed, as illustrated in Figure 9. Select the HPG User role from the [Select a Role] drop down menu.

Figure 9: Select a Role



The page indicates that the selected HPG User role requires Identity Verification, as illustrated in Figure 10. Select [Next] to continue.

Figure 10: HPG User Role Identity Verification



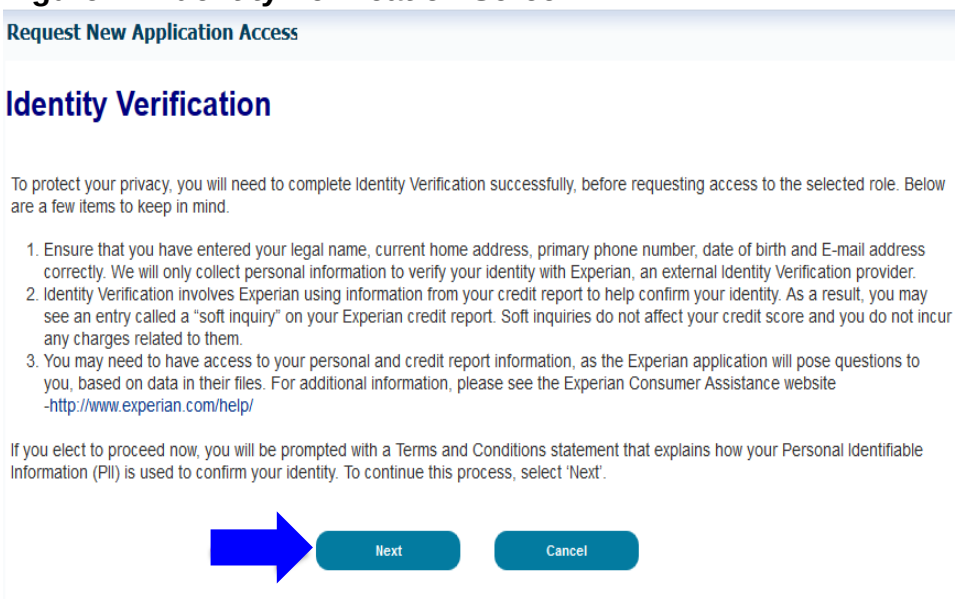
13. Depending on your CMS Enterprise Portal account, you may now be directed to the ***Identify Verification*** page, as illustrated in Figure 11. This identify verification process (Remote Identity Proofing or RIDP) is used to verify your identity and is done by asking questions based on your personal 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.

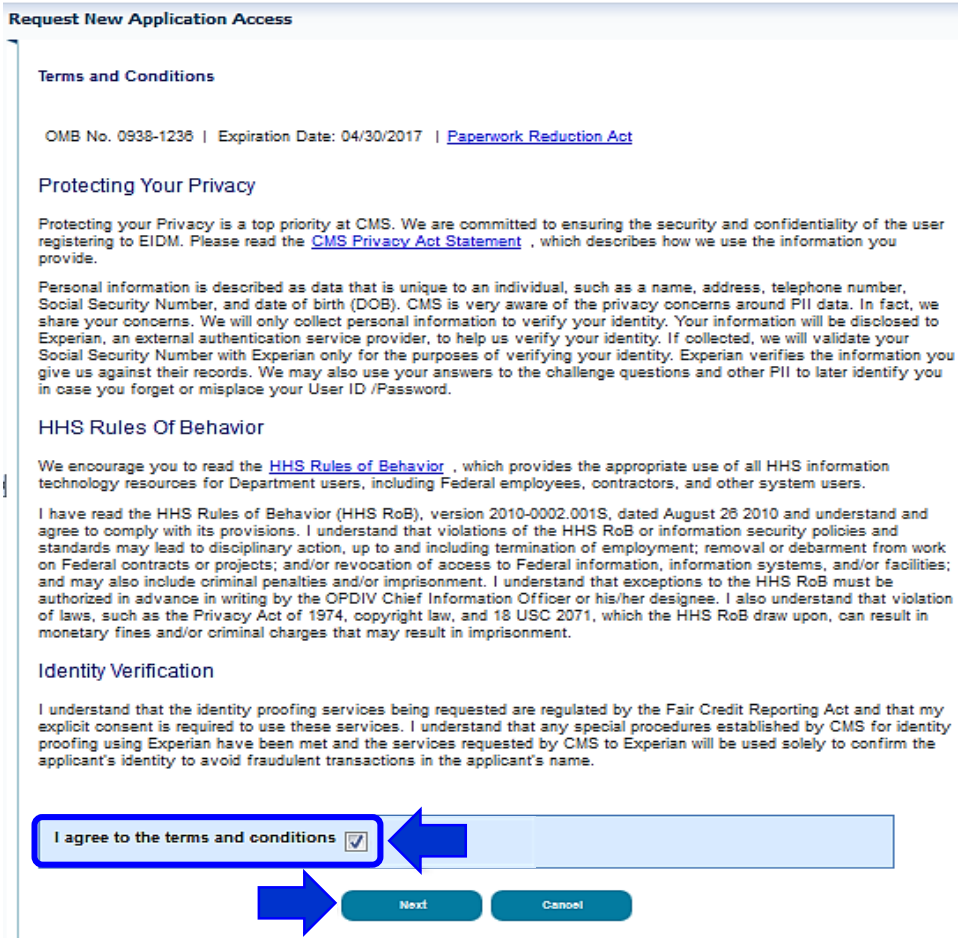
Figure 11: Identity Verification Screen



14. Read the ***Terms and Conditions***, as illustrated in Figure 12. 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 12: Terms and Conditions Screen



Request New Application Access

Terms and Conditions

OMB No. 0938-1236 | Expiration Date: 04/30/2017 | Paperwork Reduction Act

Protecting Your Privacy

Protecting your Privacy is a top priority at CMS. We are committed to ensuring the security and confidentiality of the user registering to EIDM. Please read the CMS Privacy Act Statement , which describes how we use the information you provide.

Personal information is described as data that is unique to an individual, such as a name, address, telephone number, Social Security Number, and date of birth (DOB). CMS is very aware of the privacy concerns around PII data. In fact, we share your concerns. We will only collect personal information to verify your identity. Your information will be disclosed to Experian, an external authentication service provider, to help us verify your identity. If collected, we will validate your Social Security Number with Experian only for the purposes of verifying your identity. Experian verifies the information you give us against their records. We may also use your answers to the challenge questions and other PII to later identify you in case you forget or misplace your User ID /Password.

HHS Rules Of Behavior

We encourage you to read the HHS Rules of Behavior , which provides the appropriate use of all HHS information technology resources for Department users, including Federal employees, contractors, and other system users.

I have read the HHS Rules of Behavior (HHS RoB), version 2010-0002.001S, dated August 26 2010 and understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on Federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities; and may also include criminal penalties and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the OPDIV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

Identity Verification

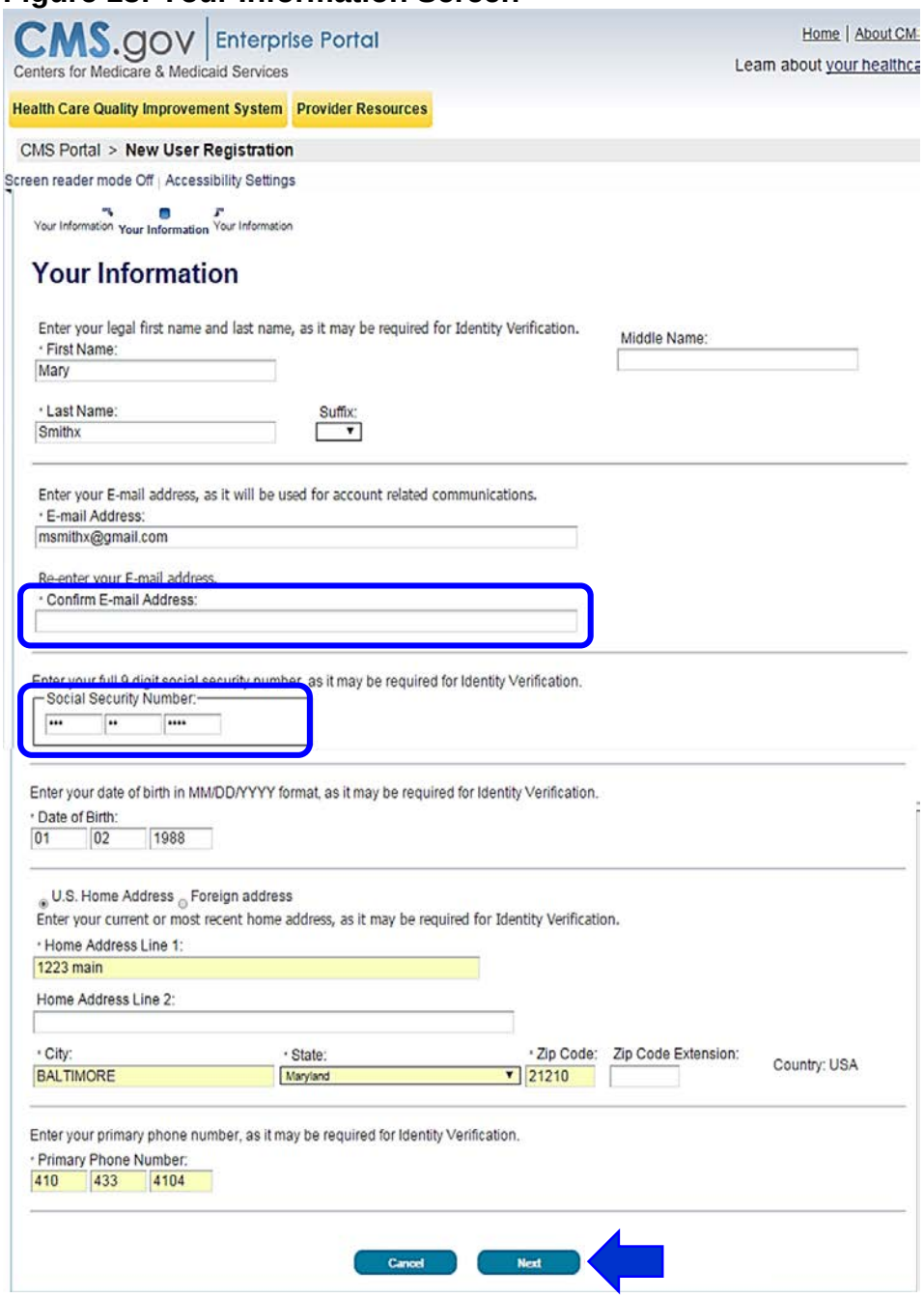
I understand that the identity proofing services being requested are regulated by the Fair Credit Reporting Act and that my explicit consent is required to use these services. I understand that any special procedures established by CMS for identity proofing using Experian have been met and the services requested by CMS to Experian will be used solely to confirm the applicant's identity to avoid fraudulent transactions in the applicant's name.

I agree to the terms and conditions

Next Cancel

15. Confirm your email address and enter your Social Security Number, as illustrated in Figure 13. Verify the pre-populated information then select [Next] to continue the identity verification process.

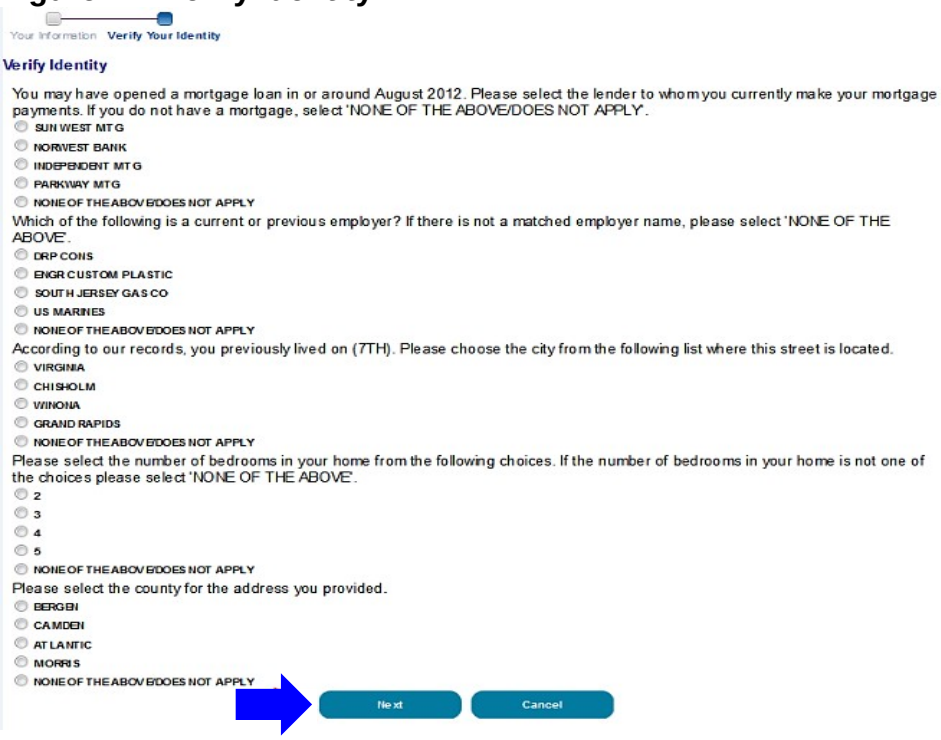
Figure 13: Your Information Screen



16. Provide an answer to each question in the ***Verify Identity*** section, as illustrated in Figure 14. 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 14: Verify Identity

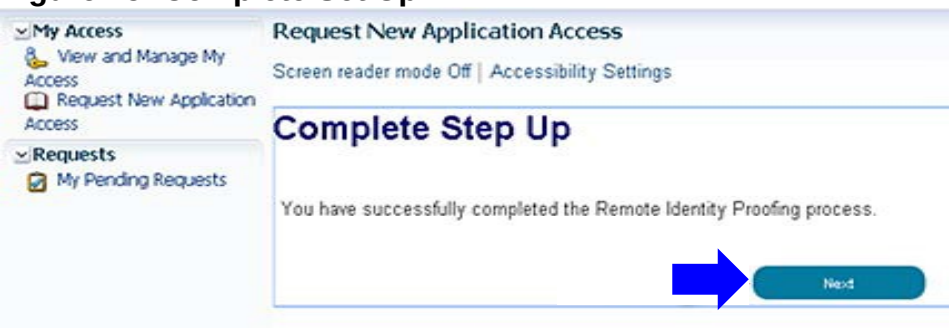


17. If the Verify Identity questions were answered properly, the Remote Identify Proofing (RIDP) process is now complete. Select [Next] to continue with the HPG User role request process, as illustrated in Figure 15.

    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 15: Complete Set Up

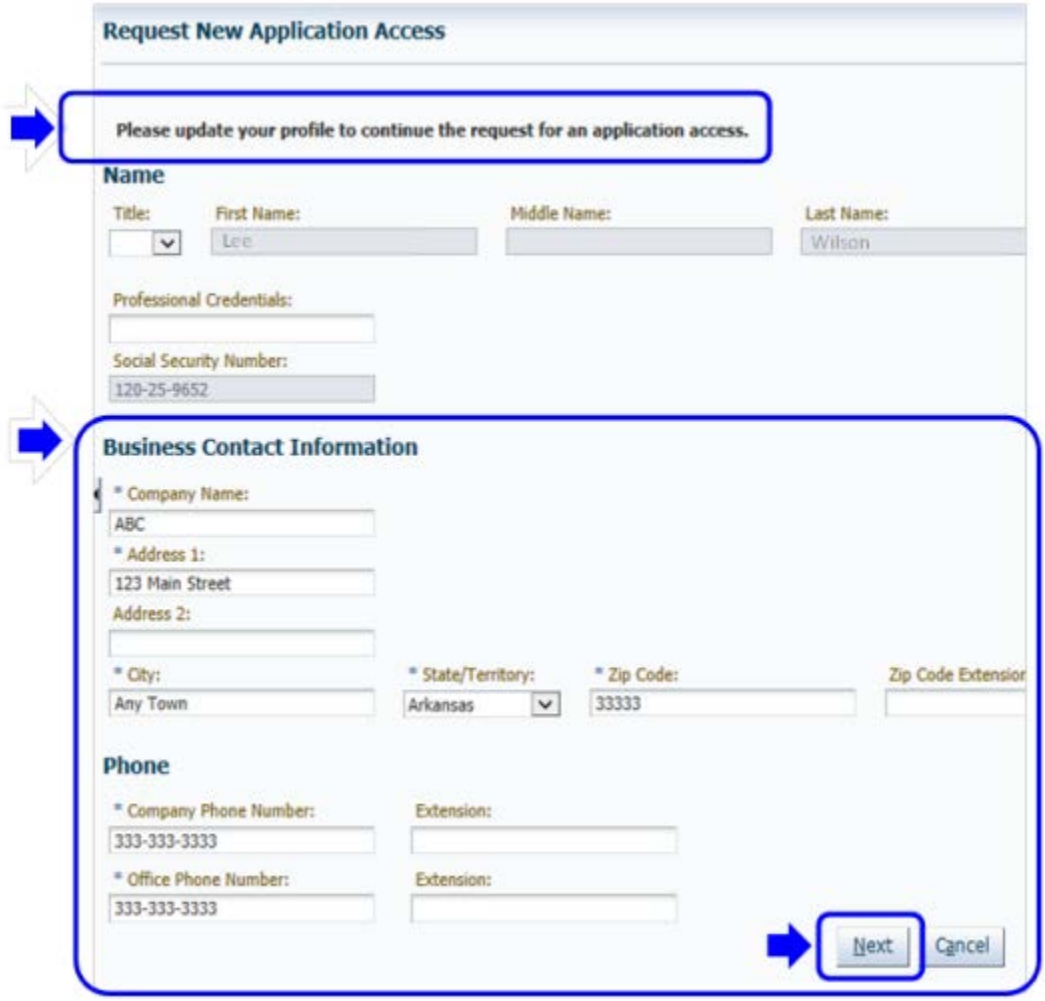


18. After completing the RIDP process, ***Request New Application*** page is displayed, as illustrated in Figure 16. If all of your required business contact information is not on file, you will have to provide this information

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.

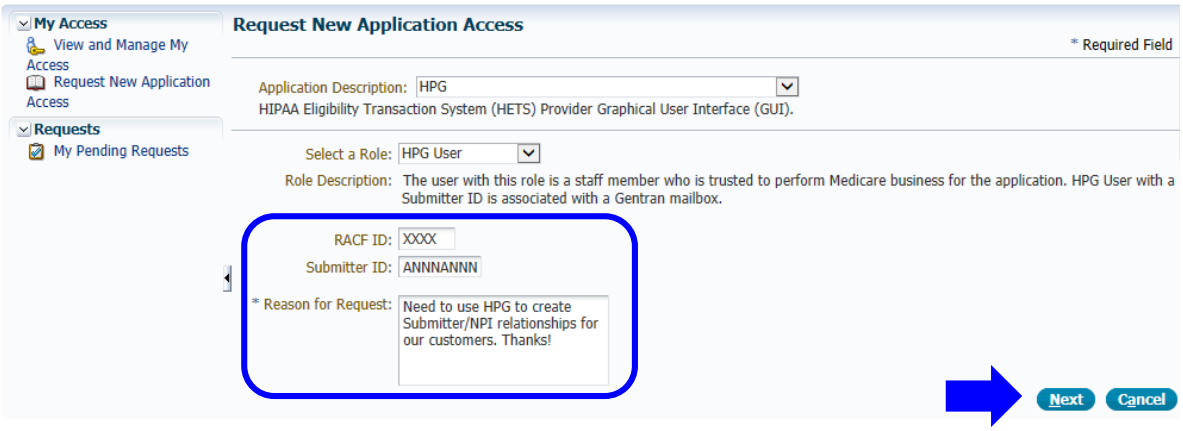
Note: If all of your business contact information is on file, the “Please update your profile…” message will not be displayed and the “Select a role” drop down menu will be displayed for you to continue. (See Step 11.) If the “Please update your profile…” message is displayed, enter the required information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

Figure 16: Request New Application Access Screen



19. 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].

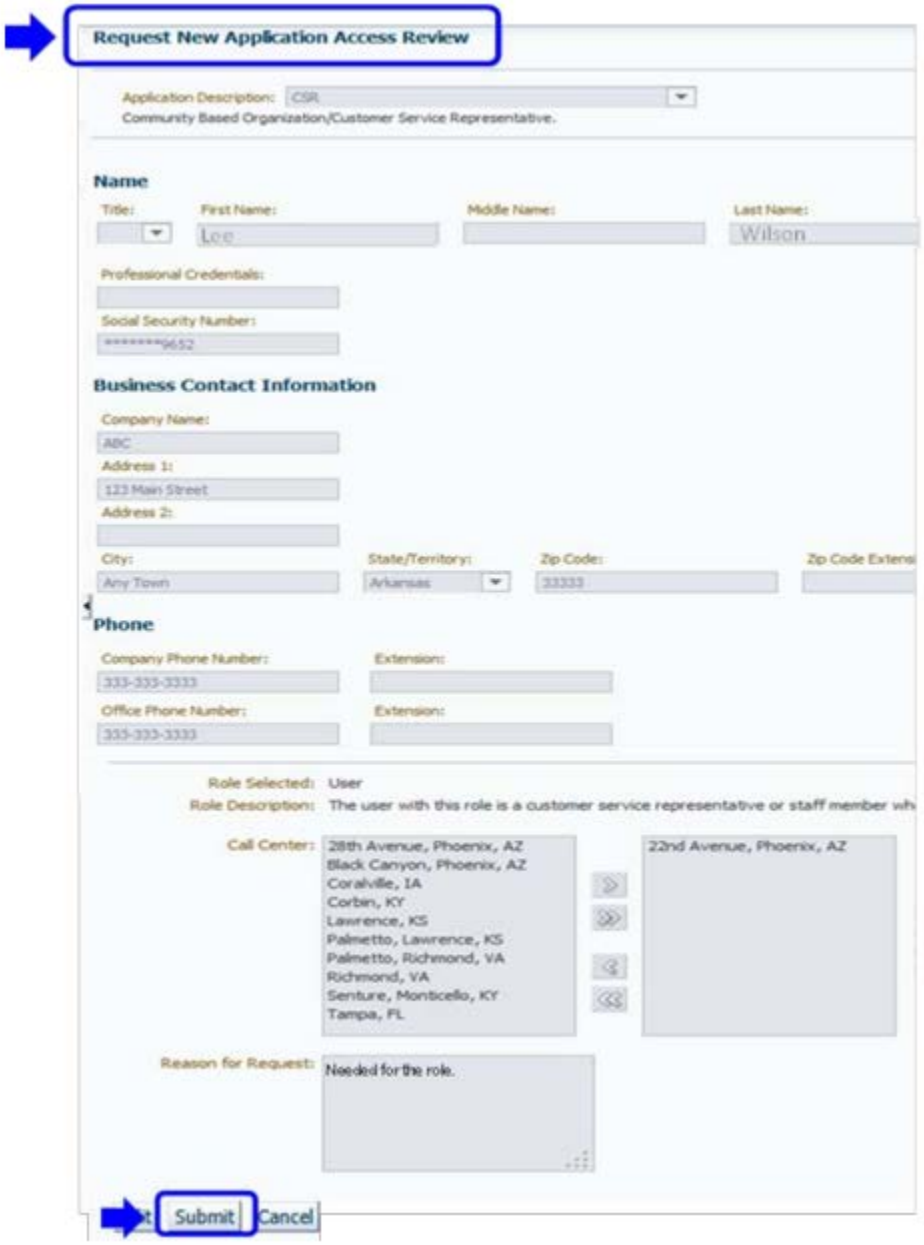
Figure 17: Provide RACF ID, Submitter ID, and Reason for Request



20. 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.

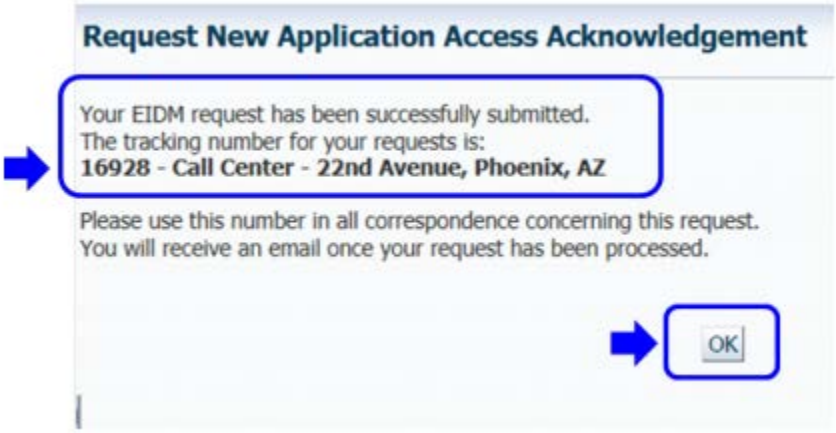
Figure 18: Request New Application Access Review



21. 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 HPG 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 HPG 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: HPG requires that all CMS Enterprise Portal User IDs be 32 alphanumeric characters or less (see Section 4.2). HPG also requires that CMS Enterprise Portal passwords contain only alphanumeric characters. 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.

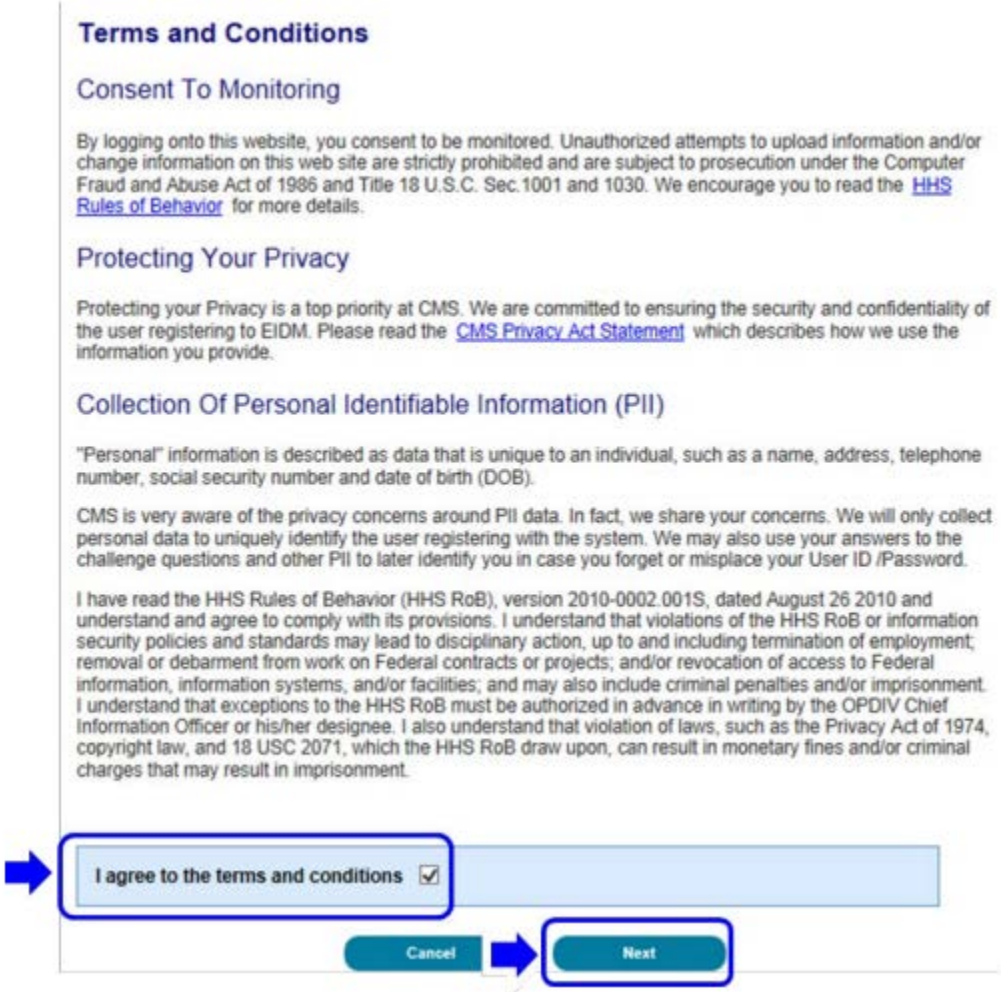
Figure 20: CMS Enterprise Portal Screen

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

Figure 21: New User Registration

3. Read the ***Terms and Conditions***, select [I agree to the terms and conditions], and then select [Next] to continue with the registration process, as illustrated in Figure 22.

Figure 22: Terms and Conditions Screen



Terms and Conditions

Consent To Monitoring

By logging onto this website, you consent to be monitored. Unauthorized attempts to upload information and/or change information on this web site are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. Sec.1001 and 1030. We encourage you to read the HHS Rules of Behavior for more details.

Protecting Your Privacy

Protecting your Privacy is a top priority at CMS. We are committed to ensuring the security and confidentiality of the user registering to EIDM. Please read the CMS Privacy Act Statement which describes how we use the information you provide.

Collection Of Personal Identifiable Information (PII)

"Personal" information is described as data that is unique to an individual, such as a name, address, telephone number, social security number and date of birth (DOB).

CMS is very aware of the privacy concerns around PII data. In fact, we share your concerns. We will only collect personal data to uniquely identify the user registering with the system. We may also use your answers to the challenge questions and other PII to later identify you in case you forget or misplace your User ID /Password.

I have read the HHS Rules of Behavior (HHS RoB), version 2010-0002.001S, dated August 26 2010 and understand and agree to comply with its provisions. I understand that violations of the HHS RoB or information security policies and standards may lead to disciplinary action, up to and including termination of employment; removal or debarment from work on Federal contracts or projects; and/or revocation of access to Federal information, information systems, and/or facilities; and may also include criminal penalties and/or imprisonment. I understand that exceptions to the HHS RoB must be authorized in advance in writing by the OPDIV Chief Information Officer or his/her designee. I also understand that violation of laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS RoB draw upon, can result in monetary fines and/or criminal charges that may result in imprisonment.

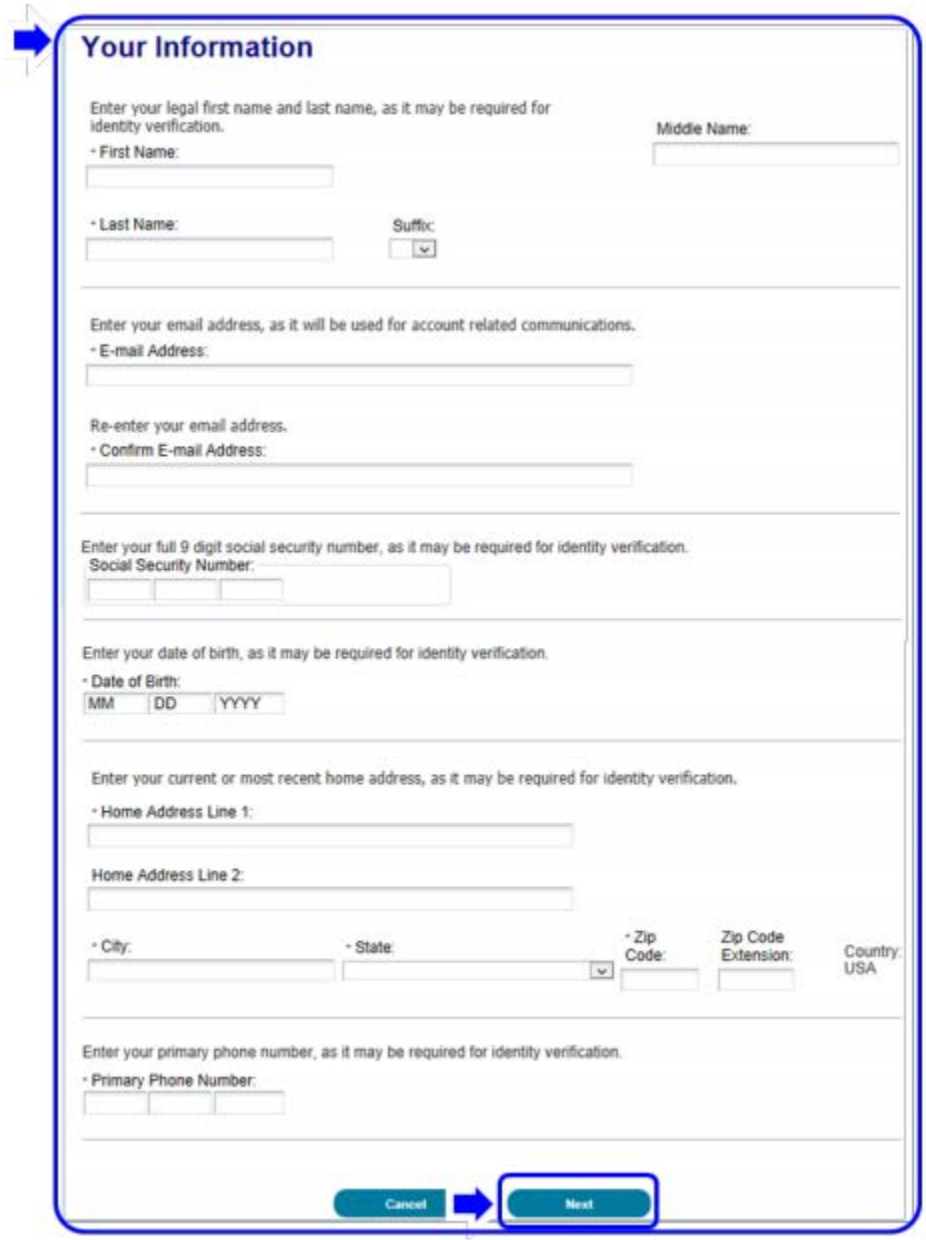
I agree to the terms and conditions ☑

Cancel Next

4. The ***Your Information*** page is displayed, as illustrated in Figure 23. Provide the information requested on the ***Your Information*** page. The fields with an asterisk (*) are required fields and have to be completed. 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 23: Your Information Screen



5. After providing the required information on the ***Your Information*** page, the ***Choose User ID and Password*** page is displayed, as illustrated in Figure 24. 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 HPG requires that all CMS Enterprise Portal User IDs be 32 alphanumeric characters or less (see Section 4.2).

Figure 24: Choose User ID and Password

6. Create and enter a password of your choice, as illustrated in Figure 25.

   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: HPG requires that CMS Enterprise Portal passwords contain only alphanumeric characters.

   Note: The passwords must match before you can continue.

Figure 25: Create and Confirm Password

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, as illustrated in Figure 26. Continue to select a question and to enter an answer for Question 2 and Question 3. Select [Next] to complete the registration process.

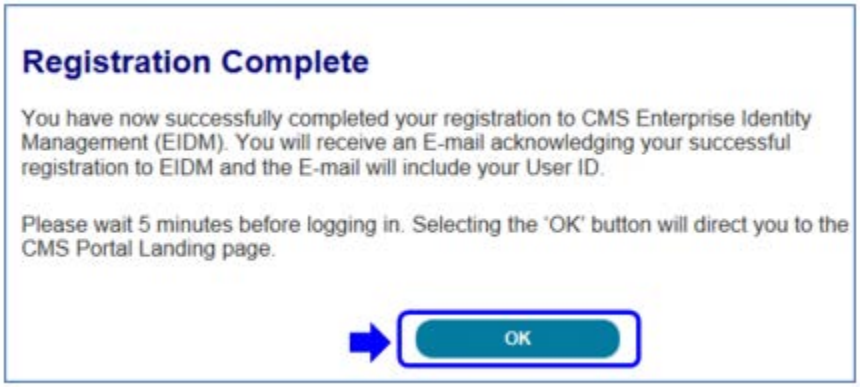
Note: You may select Cancel to exit out of the User ID registration process. All information provided, and any changes made, will not be saved. In the example below, select Next to complete the registration process.

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

Figure 26: Select Challenge Questions and Answers

8. After selecting [Next], the ***Registration Complete*** page is displayed, as illustrated in Figure 27. The ***Registration Complete*** page informs you that you will receive an email acknowledging your successful registration and will include your User ID. Select [OK] to close the ***Registration Complete*** page.

Figure 27: Registration Complete



9. After creating your CMS Enterprise Portal User ID and password, follow the steps outlined in Section 4.3.1 to add the HPG 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 HPG) 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 be able to receive text messaging (SMS); or you should have a valid email address.

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

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

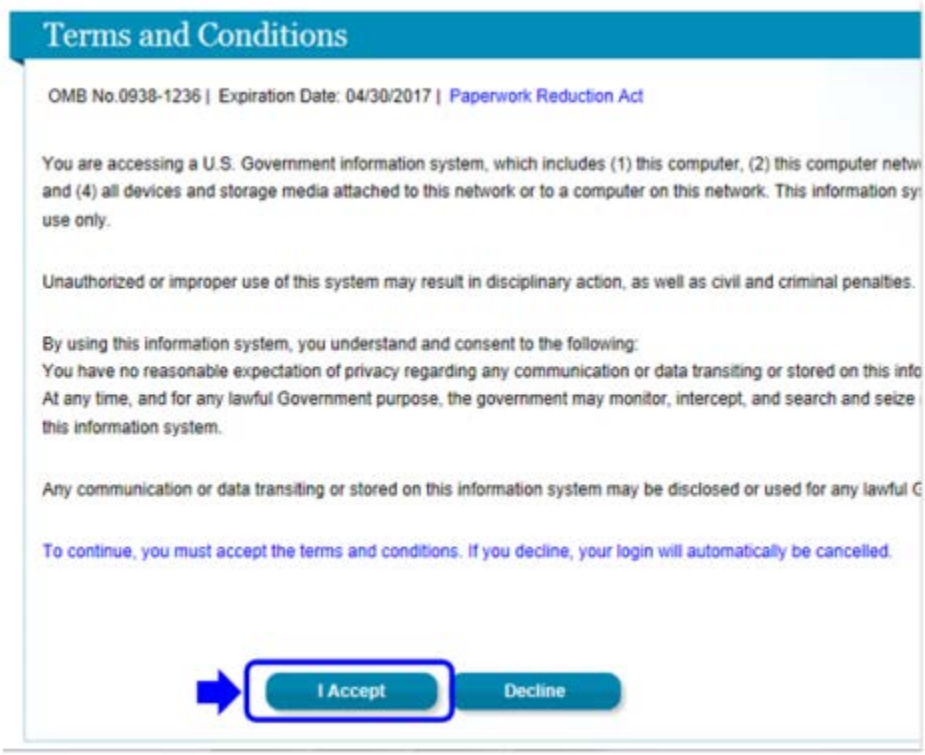
Figure 28: CMS Enterprise Portal Screen

2. Select [Login to CMS Secure Portal], as illustrated in Figure 29.

Figure 29: Login to CMS Secure Portal

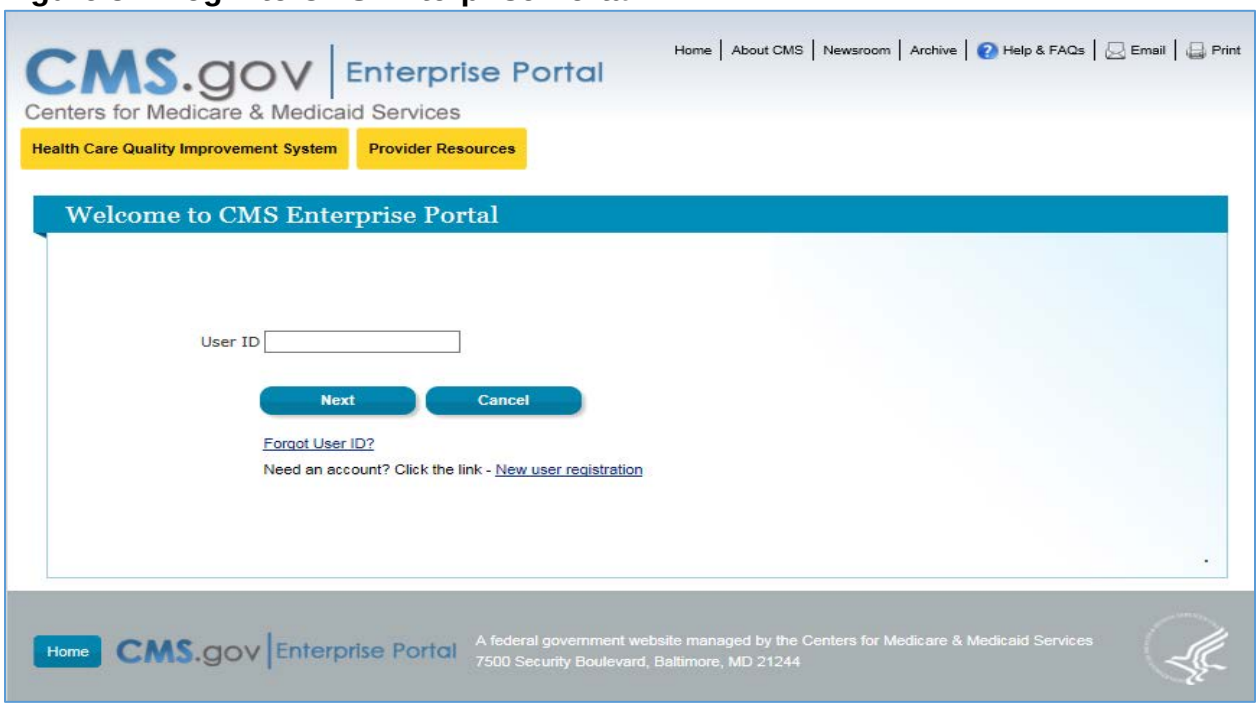
3. Read the Terms and Conditions and select [I Accept] to continue with the registration process, as illustrated in Figure 30.

Figure 30: Terms and Conditions Screen



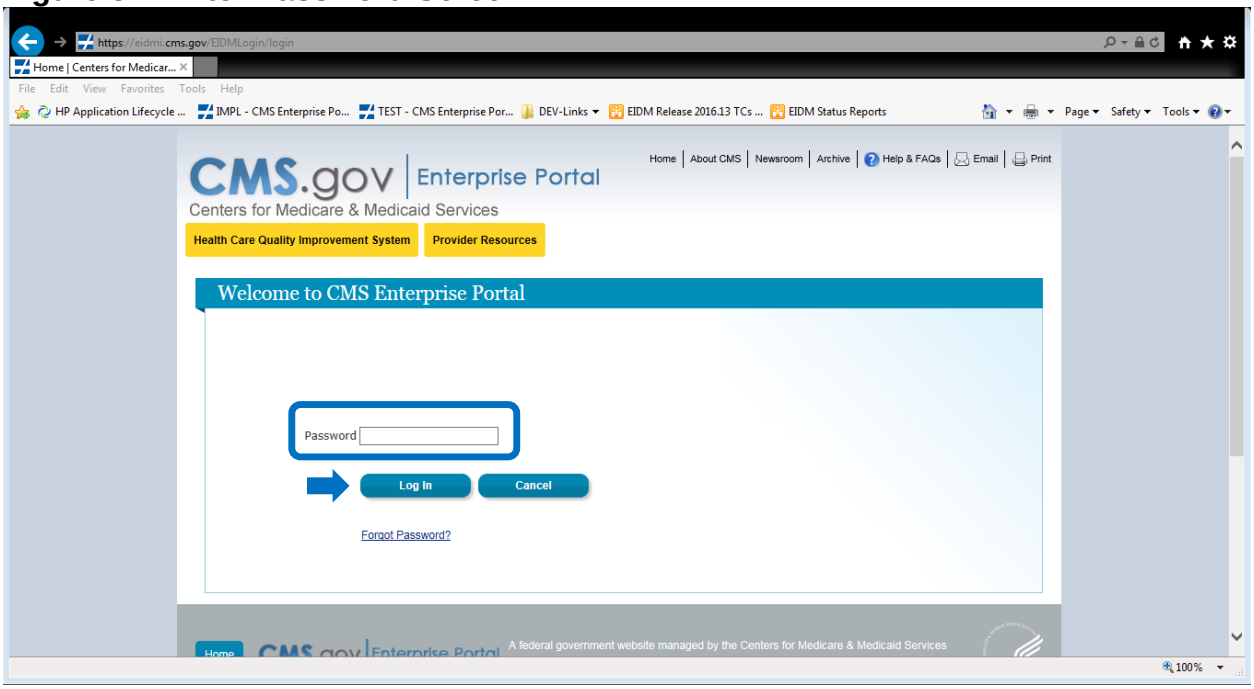
4. Enter your CMS Enterprise Portal User ID and select [Next] to log in, as illustrated in Figure 31.

Figure 31: Login to CMS Enterprise Portal



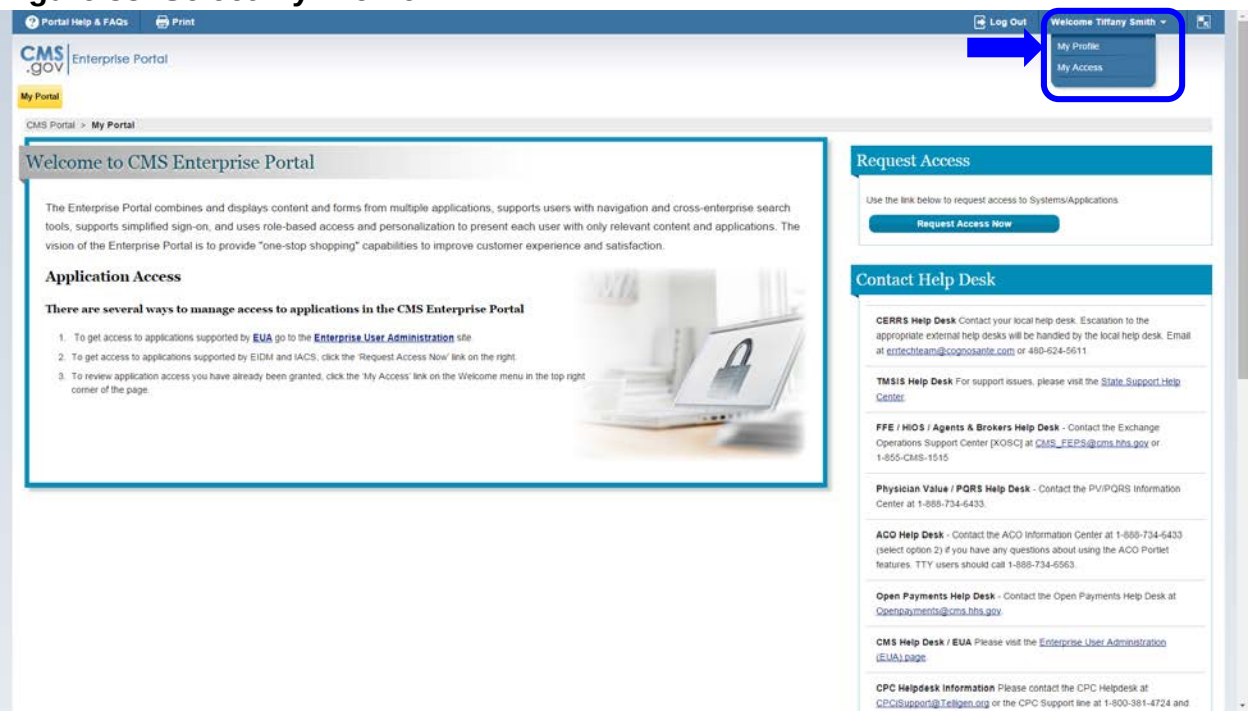
5. The Enter Password Screen will display as illustrated in Figure 32. Enter the CMS Enterprise Portal password then select [Log In].

Figure 32: Enter Password Screen



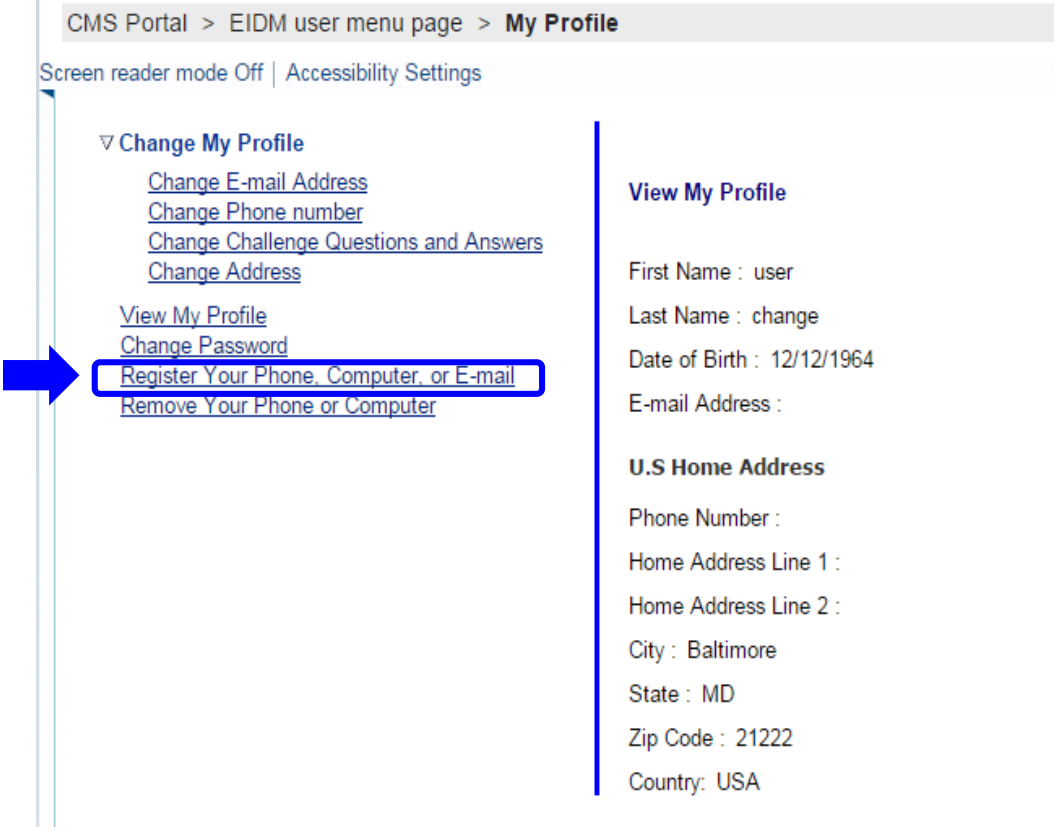
6. Select your username and then select [My Profile] from the dropdown menu to go to your profile, as illustrated in Figure 33.

Figure 33: Select My Profile



7. Select [Register Your Phone, Computer, or Email] from the navigation links on the left to begin the process of adding MFA to your account, as illustrated in Figure 34.

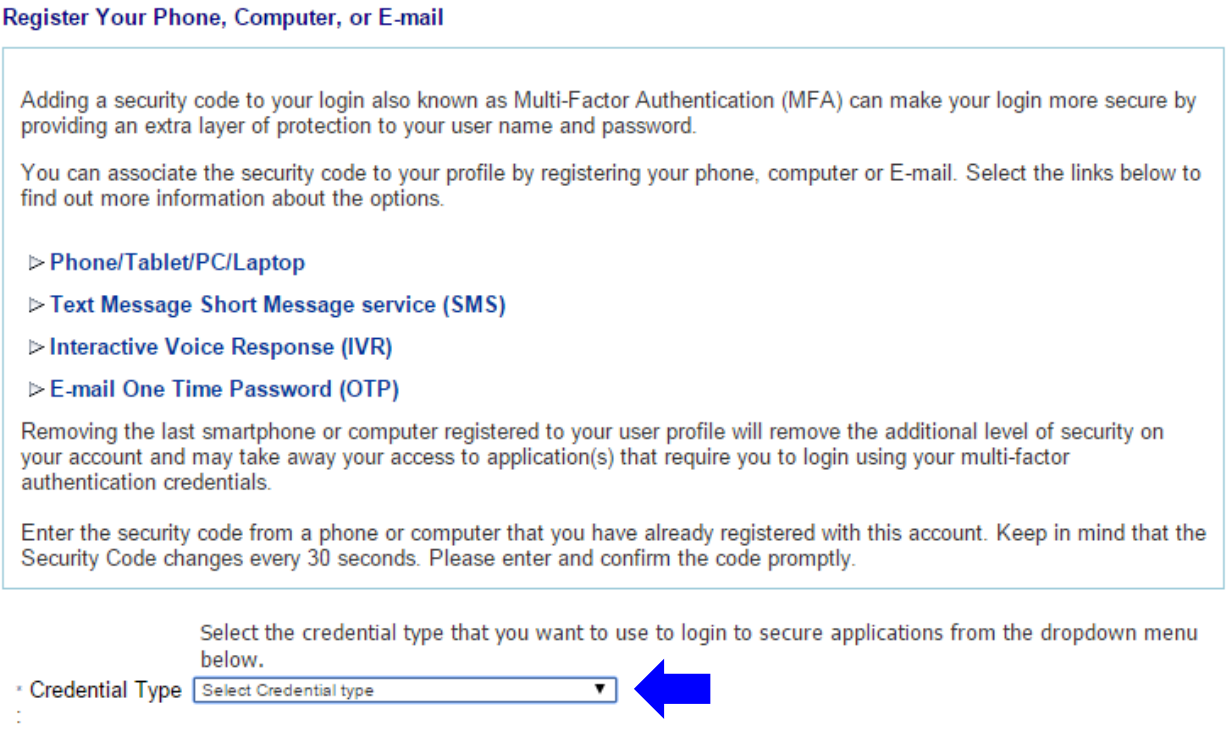
Figure 34: Register Phone, Computer, or Email



8. Read the Register Your Phone, Computer or Email page notification, as illustrated in Figure 35. 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 30 seconds to retrieve and enter the MFA security code. If you are unable to enter the MFA security code within 30 seconds, then the code will expire and you will need to request a new security code.

Figure 35: Select Credential Type



9. (a) Phone/Tablet/PC/Laptop. If selecting [Phone/Tablet/PC/Laptop] as [Credential Type], enter the alphanumeric code that displays in the Symantec VIP Access Credential ID field, illustrated in Figure 36, into the Credential ID field, as illustrated in Figure 37. Enter a brief description in the field labeled [Credential Description] (i.e., “work laptop”).

Figure 36: Symantec Credential ID

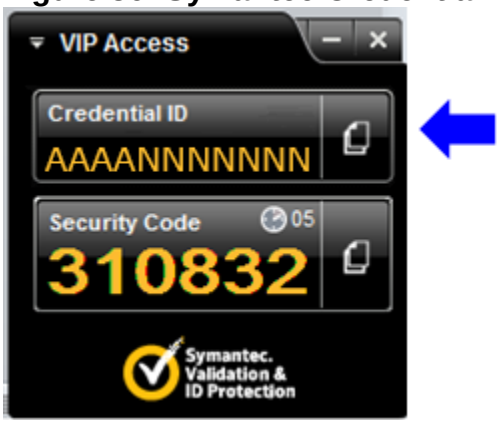
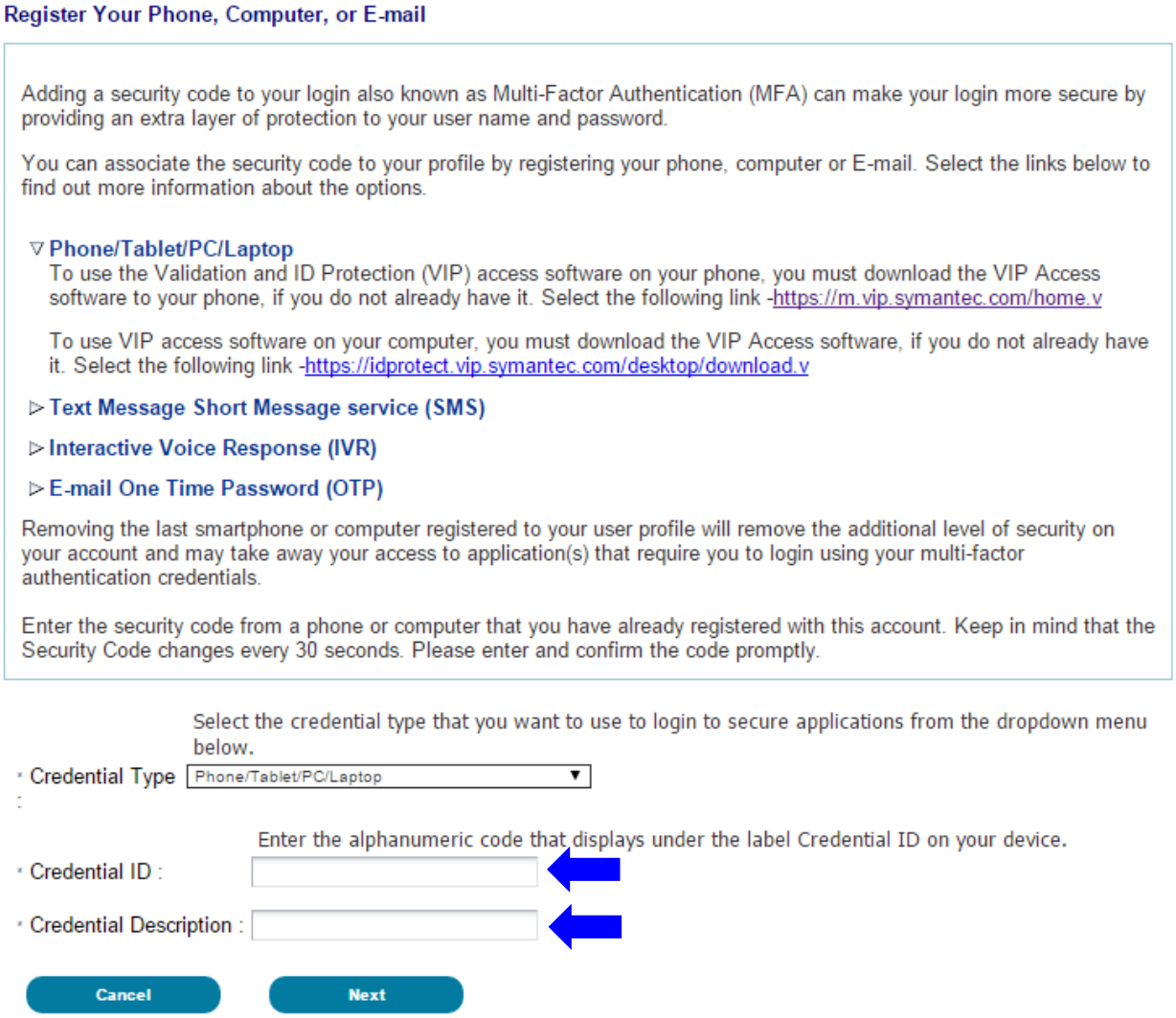
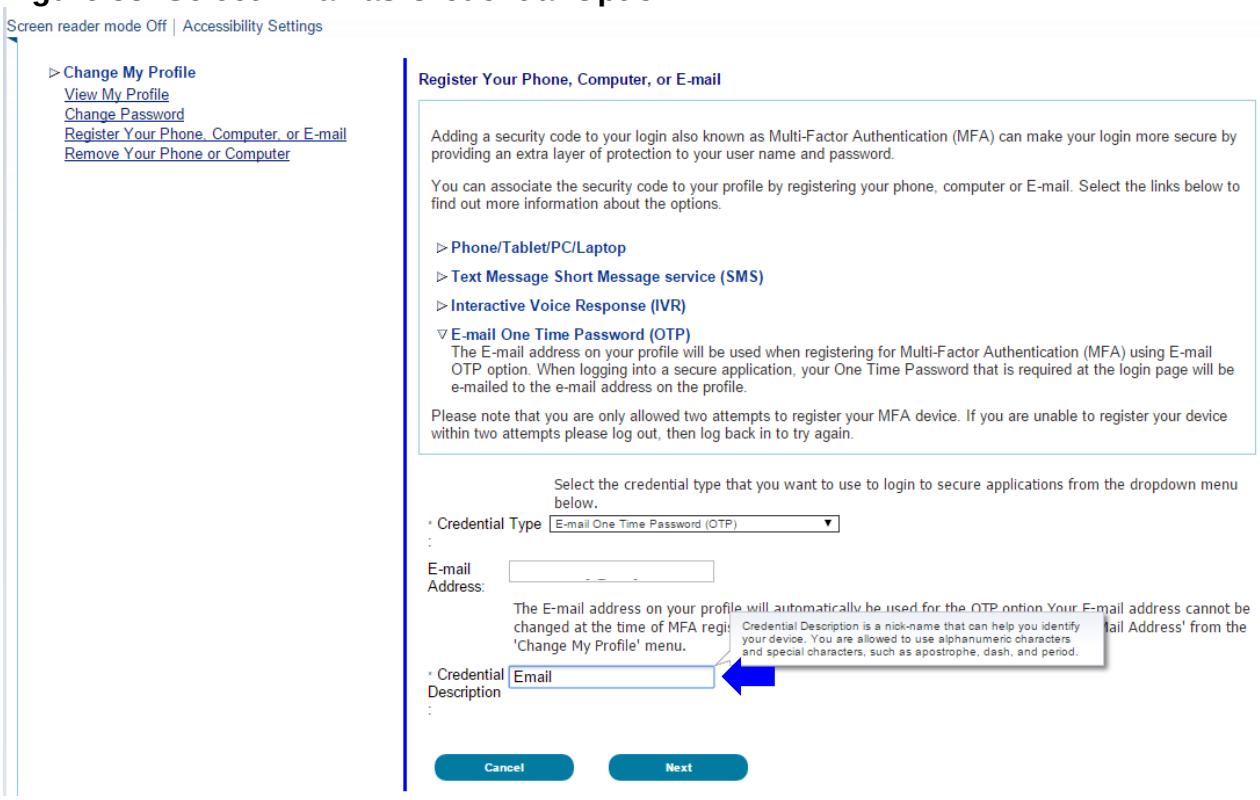


Figure 37: Select Phone/Tablet/PC/Laptop as Credential Option



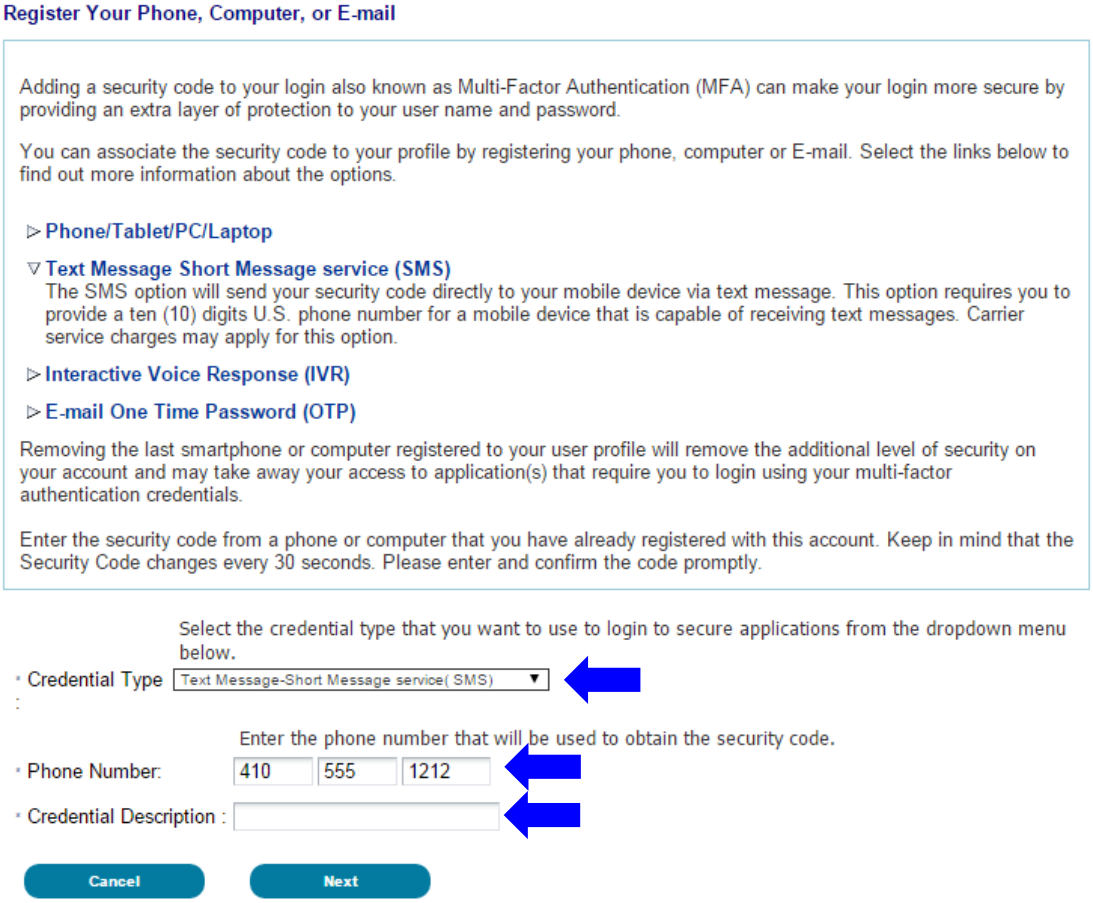
(b) Email – One Time Password (OTP). If selecting [Email – One Time Password (OTP)] as [Credential Type], the email associated with your CMS Enterprise Portal account should be entered in the field labeled [Email Address] to obtain the one time use security code. Enter [Email] as the Credential Option, as illustrated in Figure 38.

Figure 38: Select Email as Credential Option



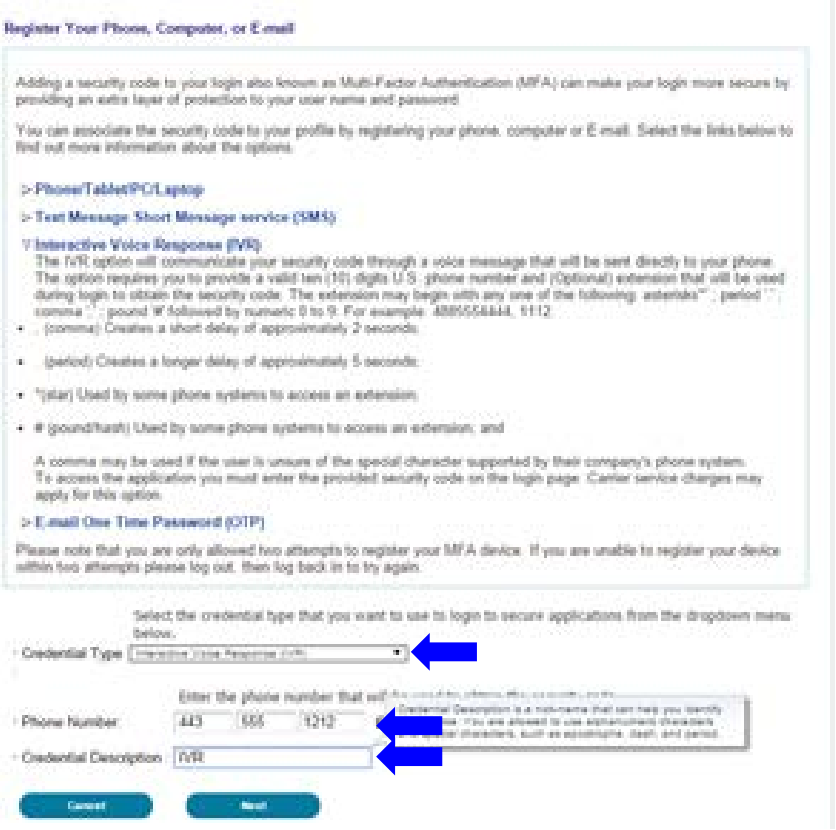
(c) Text Message – Short Message Service (SMS). If selecting [Text Message – Short Message Service (SMS)] as [Credential Type], enter the phone number that will be used to obtain the security code as [Phone Number] and [Text] as the Credential Option, as illustrated in Figure 39.

Figure 39: 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 40.

Figure 40: Select IVR as Credential Option

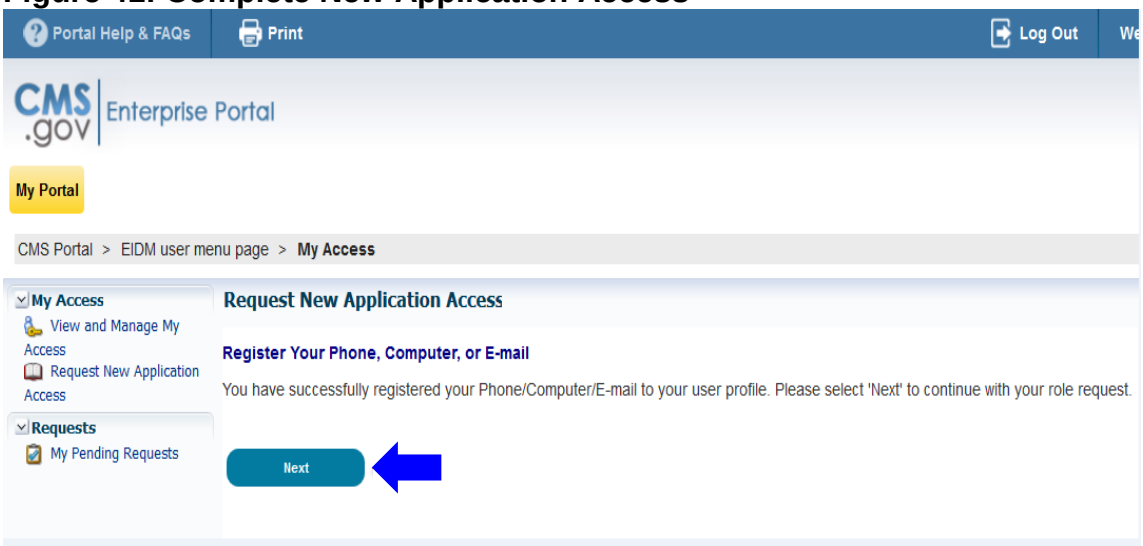


Select [Next] to continue.

10. Your registration for Multi-Factor Authentication is now complete. Select [Next] to continue, as illustrated in Figure 41.

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

Figure 41: Complete New Application Access



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 7, select [Unable to Access Security Code?]. A pop-up window is displayed, as illustrated in Figure 42.

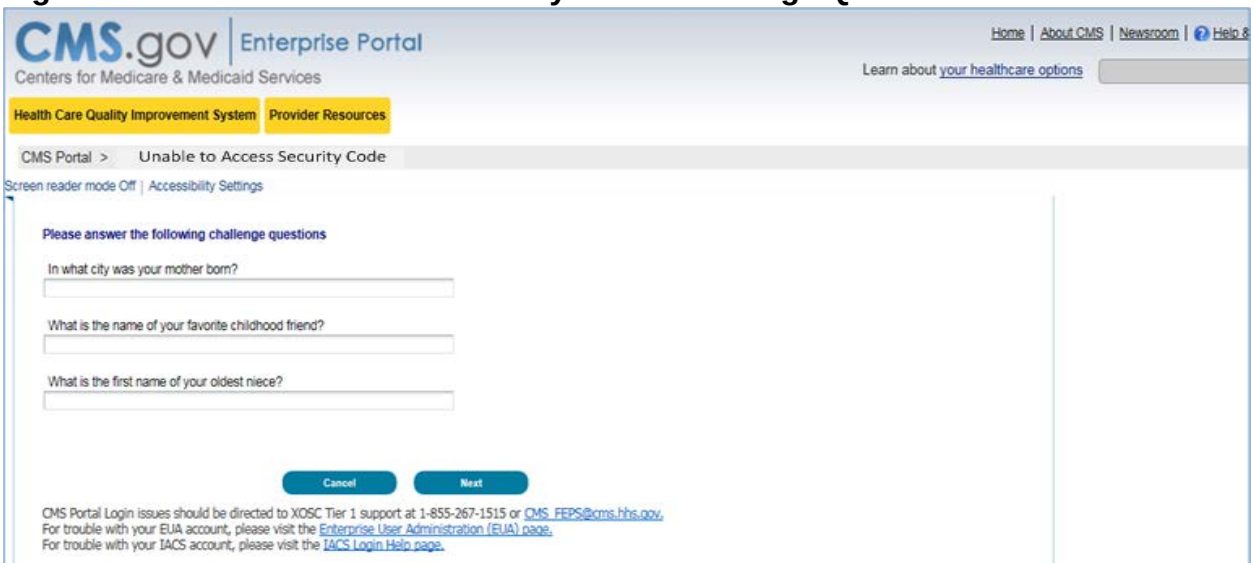
Figure 42: Unable to Access Security Code Begin Navigation

2. Select [OK]. The Unable to Access Security Code self-service process begins, as illustrated in Figure 43.

Figure 43: Unable to Access Security Code User ID Entry

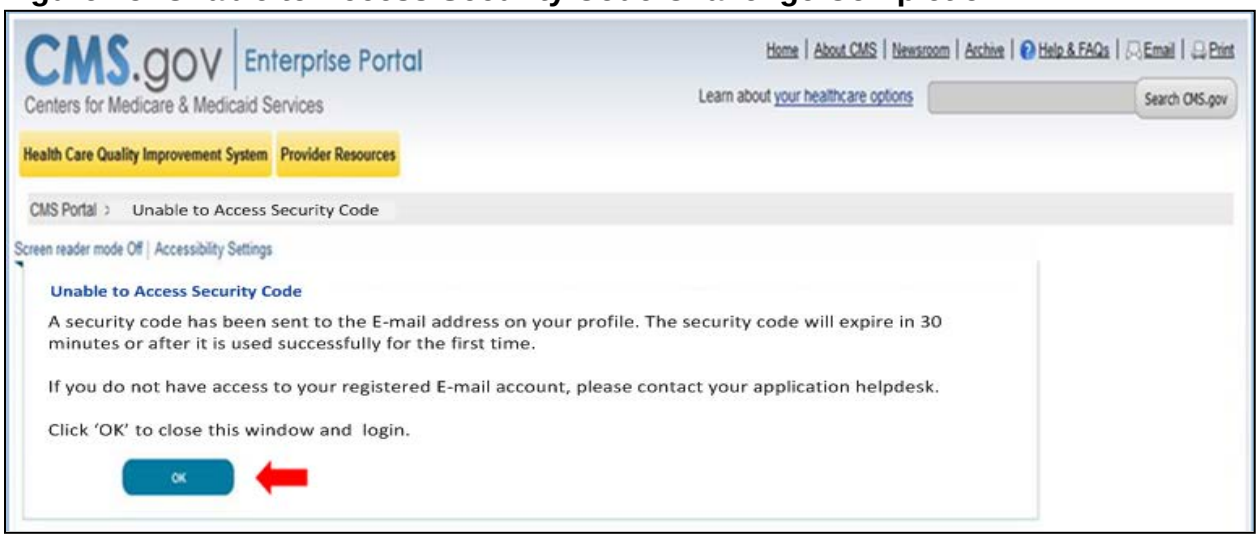
3. Enter the CMS Enterprise Portal User ID and select [Next]. The Unable to Access Security Code self-service process continues, as illustrated in Figure 44.

Figure 44: 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 [Next] to continue. The Unable to Access Security Code self-service process is completed, as illustrated in Figure 45. The CMS Enterprise Portal will send a Security Code to the User's email address on record.

Figure 45: Unable to Access Security Code Challenge Completion



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 46.

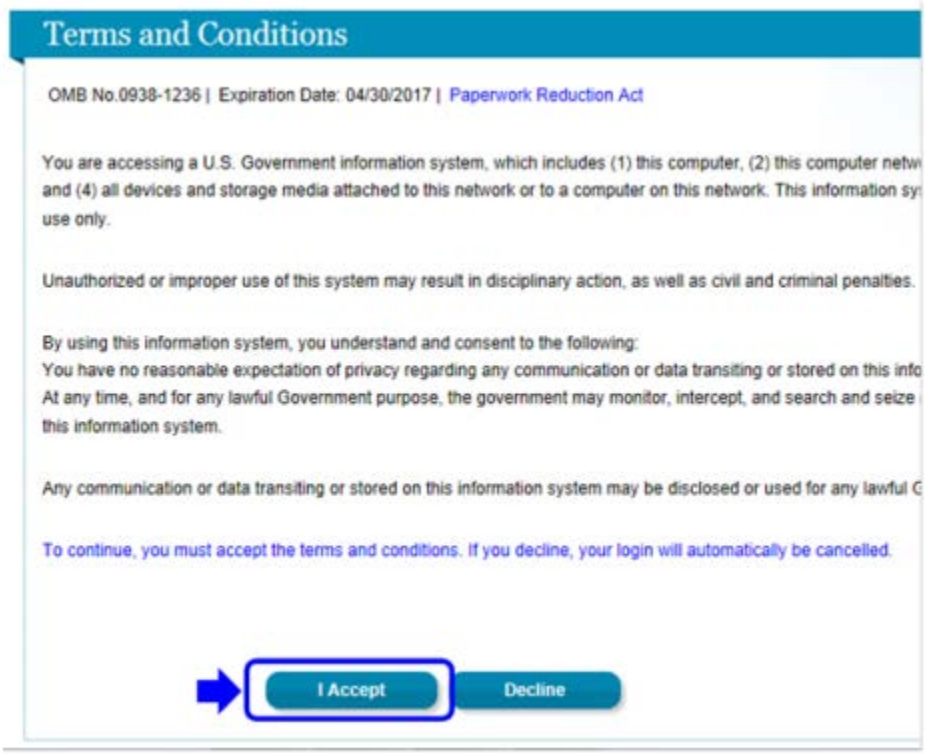
Figure 46: CMS Enterprise Portal Screen

2. Select [Login to CMS Secure Portal], as illustrated in Figure 47.

Figure 47: Login to CMS Secure Portal

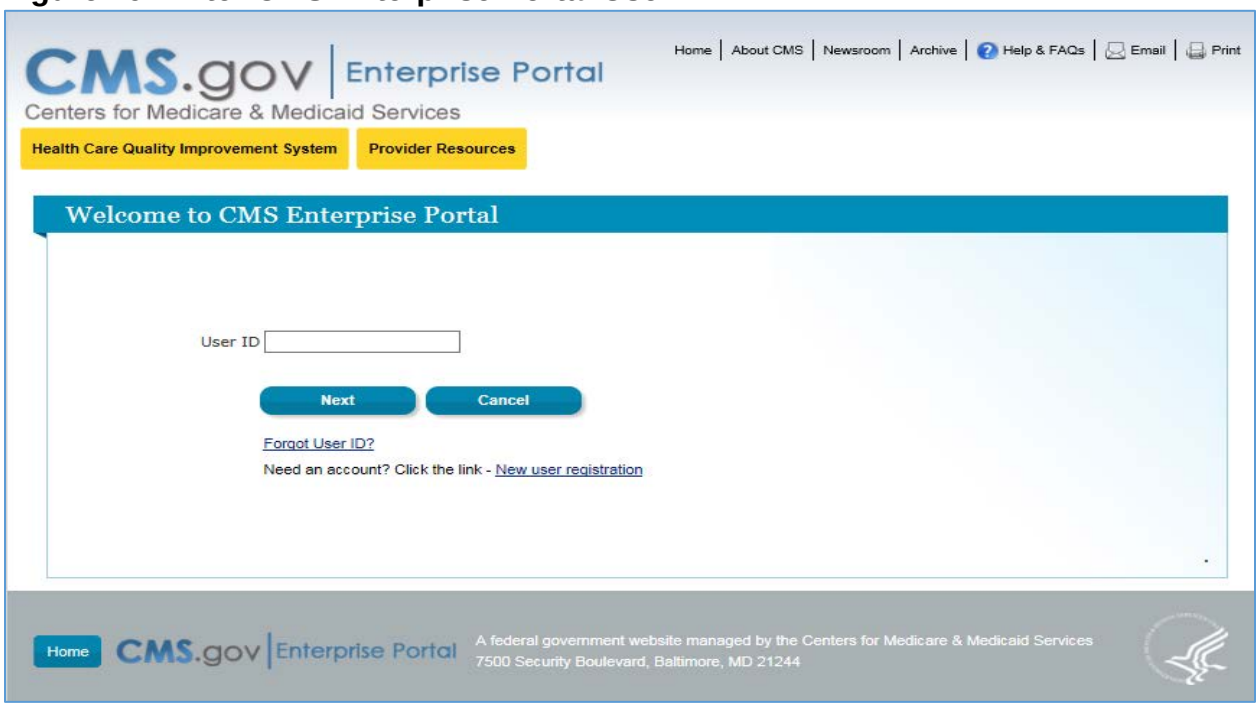
3. Read the Terms and Conditions and select [I Accept] to continue with the registration process, as illustrated in Figure 48.

Figure 48: Terms and Conditions Screen



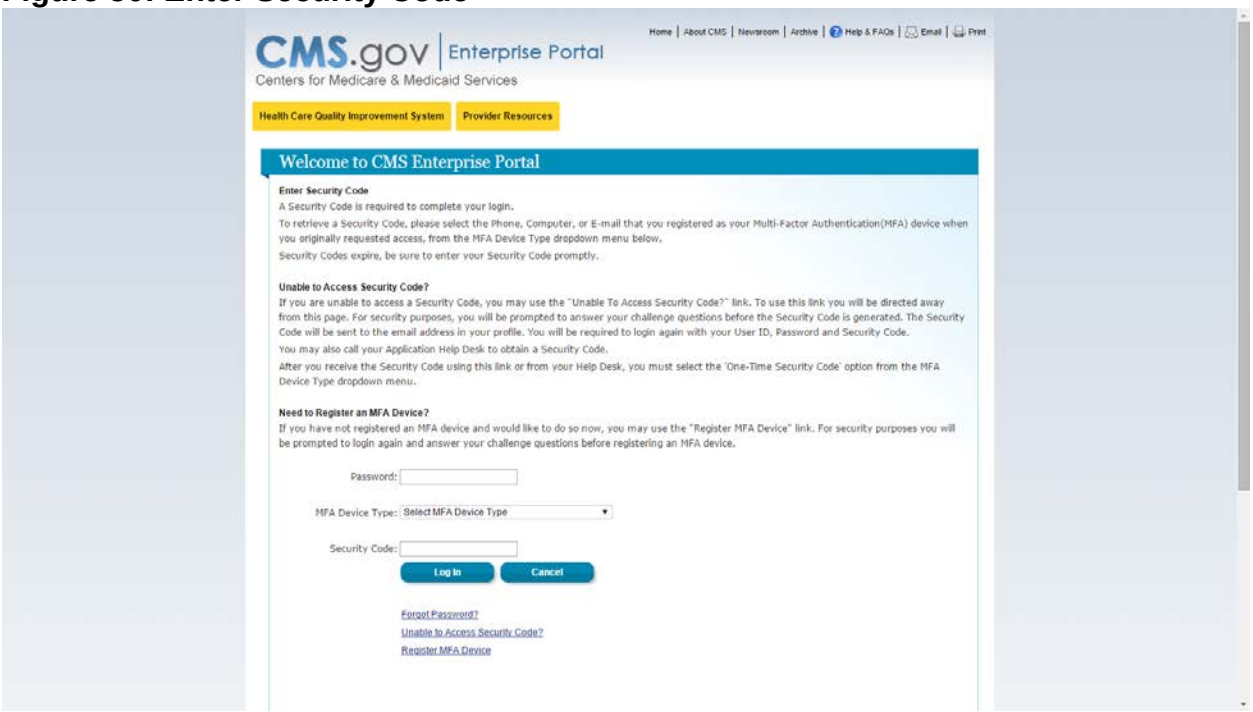
4. Enter your CMS Enterprise Portal User ID and select [Next] to log in, as illustrated in Figure 49.

Figure 49: Enter CMS Enterprise Portal User ID



5. The Enter Security Code screen will display as illustrated in Figure 50.

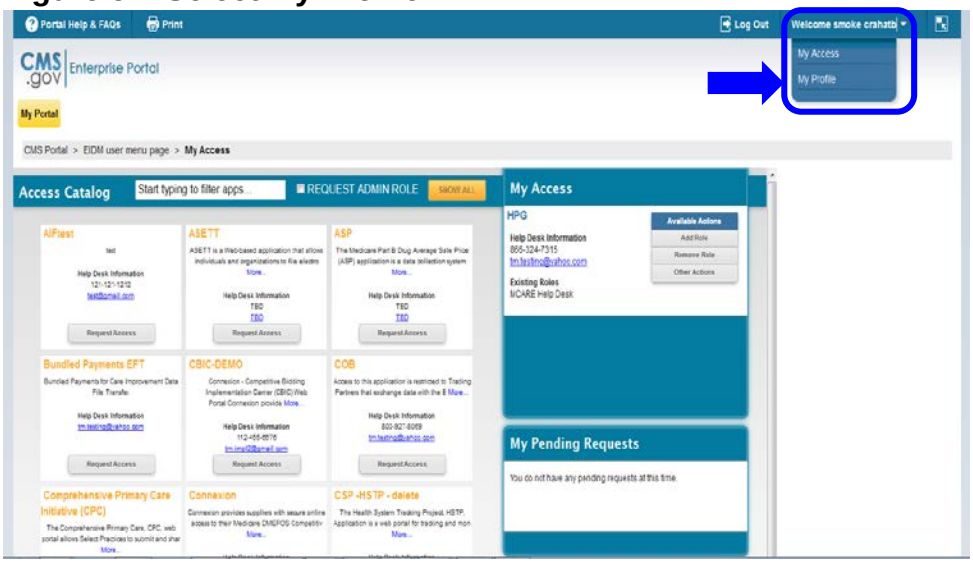
Figure 50: Enter Security Code



6. Enter your CMS Enterprise Portal password in the Password field.

7. Registered HPG 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].
8. Select your username and then select [My Profile] from the dropdown menu to go to your profile, as illustrated in Figure 51.

Figure 51: Select My Profile

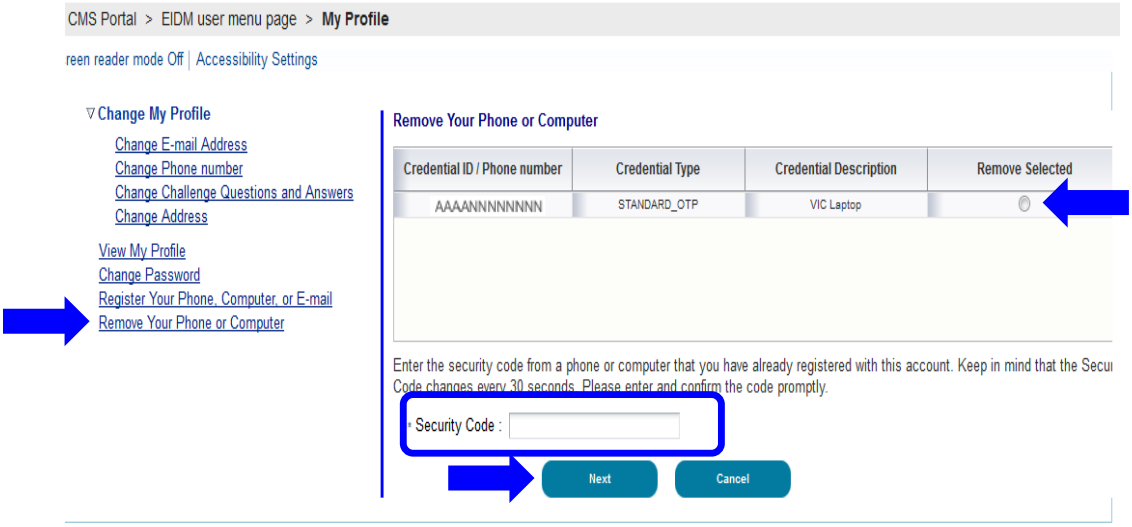


9. Select [Remove Your Phone or Computer] from the left navigation links to begin the process of removing an MFA device from your account, as illustrated in Figure 52.

   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.

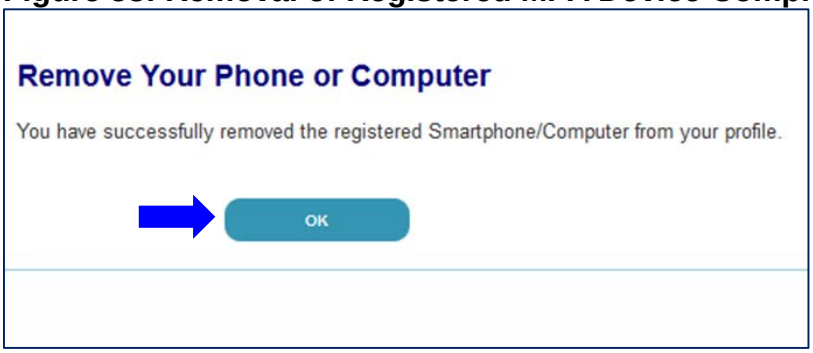
Figure 52: Remove Your Phone or Computer



10. The removal of your registered MFA device is now complete, as illustrated in Figure 53. 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 53: 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 Provider GUI (HPG) Users – existing HPG Users will not be required to complete the RIDP process. CMS uses Experian to remotely perform identity proofing.

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

The RIDP process for HPG is outlined in Section 4.3.1, steps 13-16. 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.

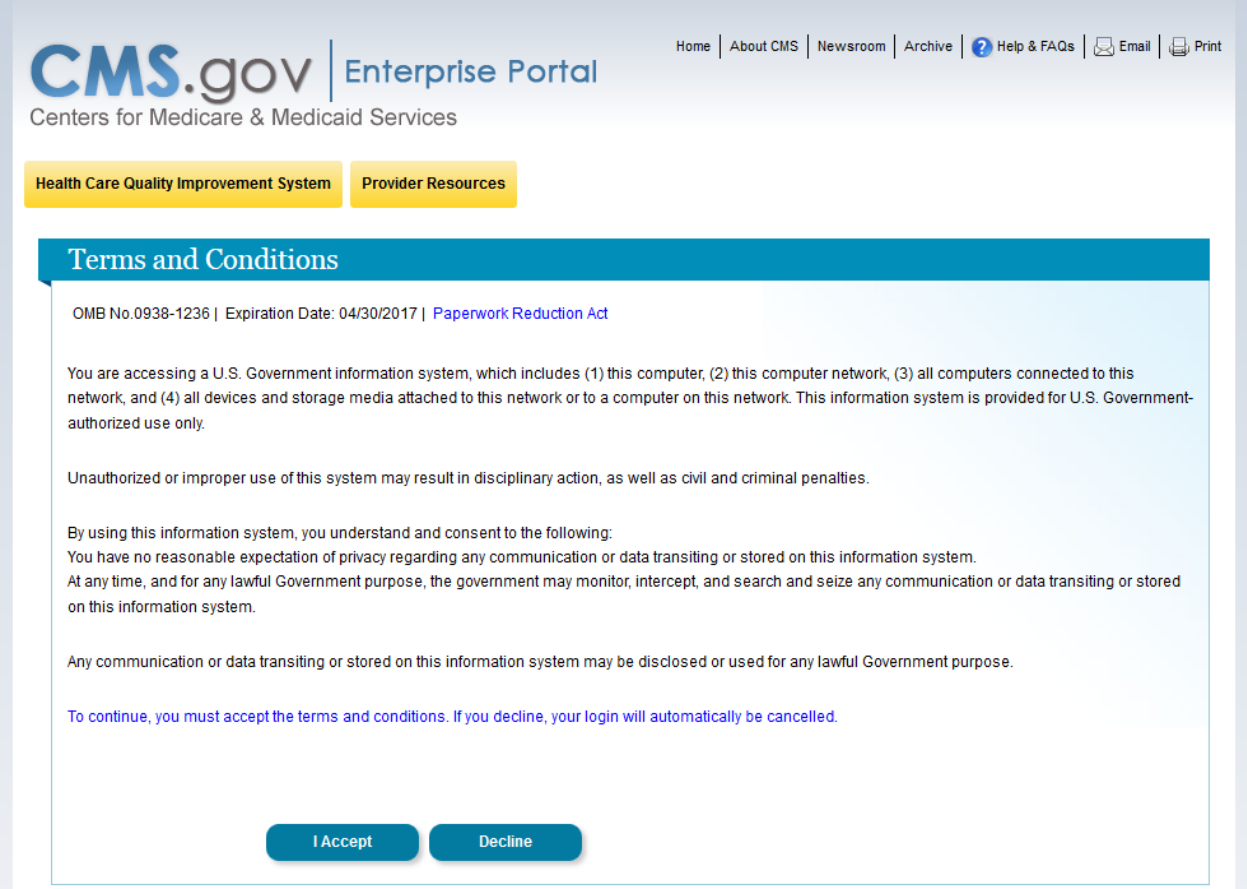
If you are asked to contact the MCARE Help Desk, you will be given a response code to help the MCARE Help Desk perform the manual identity proofing process with you. Please contact MCARE via the information provided in Section 6.5 of this guide.

4.3.6. Login to the HPG Application

Follow these steps to login to the HPG application:

1. Enter the CMS Applications Portal URL in a web browser: https://hpg.cms.hhs.gov. Please do not bookmark this or any other page in your internet browser. CMS discourages Users from utilizing browser bookmarks with the HPG application. The ***CMS Enterprise Portal Terms and Conditions*** screen will display as illustrated in Figure 54.

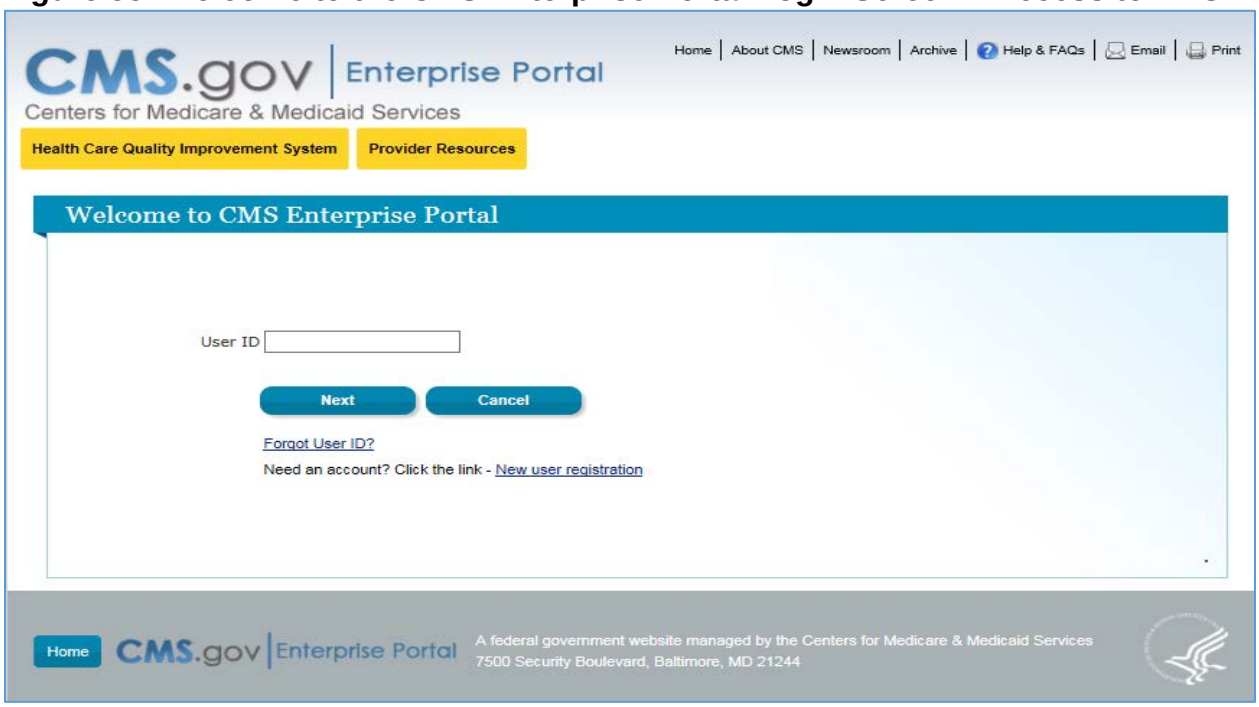
Figure 54: CMS Enterprise Portal Terms and Conditions Screen



2. Read the important information on the screen.
3. Select [I Accept] if you agree with the information on the screen. Select [Decline] if you don't want to proceed any further or if you want to exit the application.

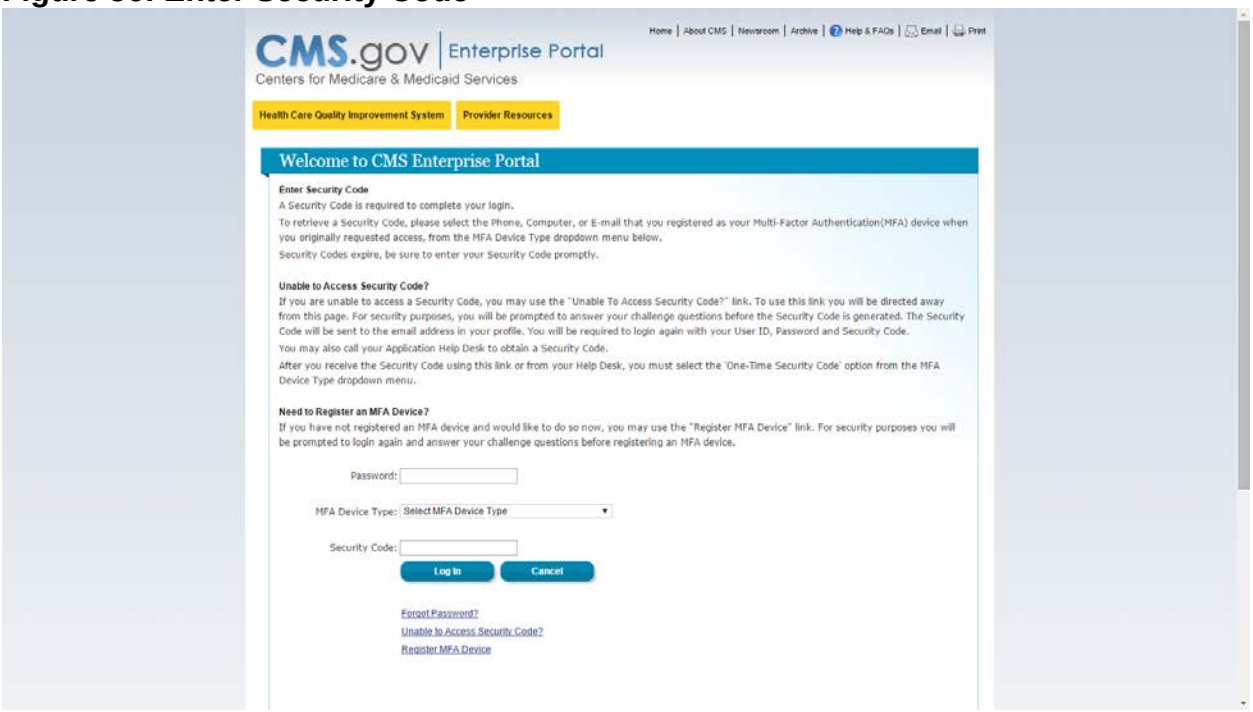
   If you select [I Accept], the ***Welcome to CMS Enterprise Portal login*** screen will display as illustrated in Figure 55 that allows authorized Users to access the HPG application.

Figure 55: Welcome to the CMS Enterprise Portal Login Screen – Access to HPG



4. Enter your CMS Enterprise Portal User ID in the **User ID** field.
5. Select [Next]. The ***Enter Security Code*** screen will display as illustrated in Figure 56.

Figure 56: Enter Security Code

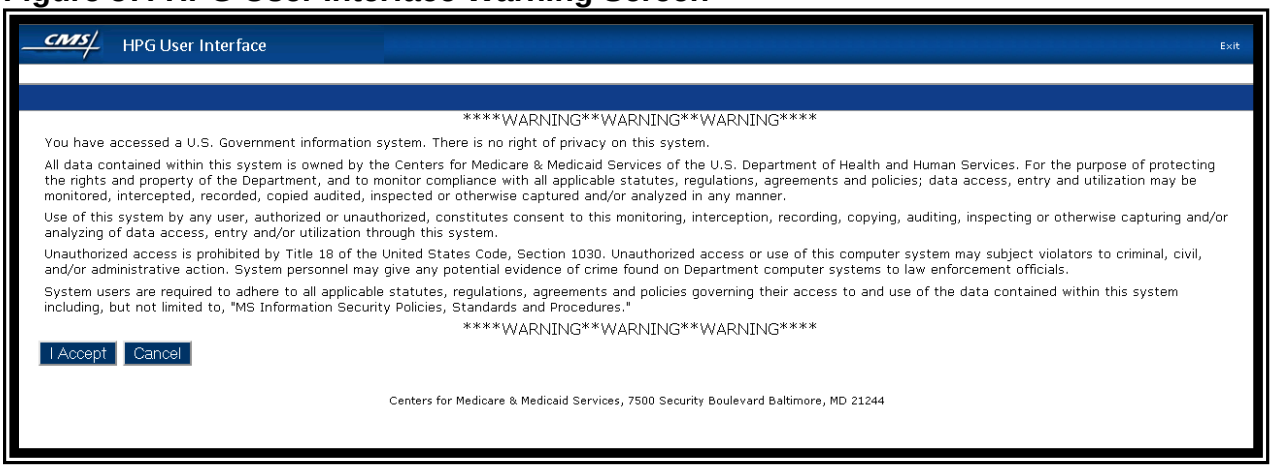


6. Enter your CMS Enterprise Portal password in the **Password** field.
7. Registered HPG Users are required to input their Multi-Factor Authentication (MFA) credentials, selecting an MFA Device that has already been associated with the CMS Enterprise Portal User ID, and then entering the appropriate 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].

   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 & HPG Password Policy. Please note that HPG 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.
8. The CMS Enterprise Portal will verify your password and MFA security code. If you are an authorized HPG user, the ***HPG User Interface Warning*** screen will display as illustrated in Figure 57.

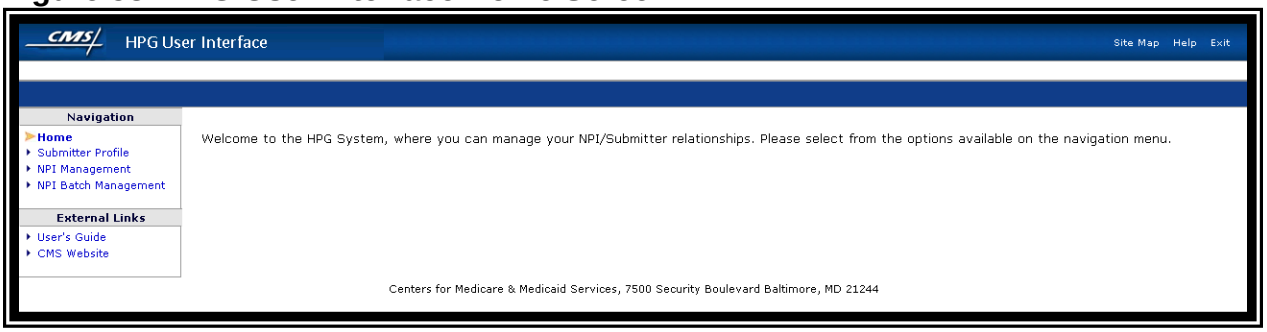
Figure 57: HPG User Interface Warning Screen



9. Read the important information on this screen.
10. Select [I Accept] if you agree with the statement. Select [Cancel] if you wish to close the application.

    If you select [I Accept], the ***HPG User Interface Home*** screen will display as illustrated in Figure 58.

Figure 58: HPG User Interface Home Screen



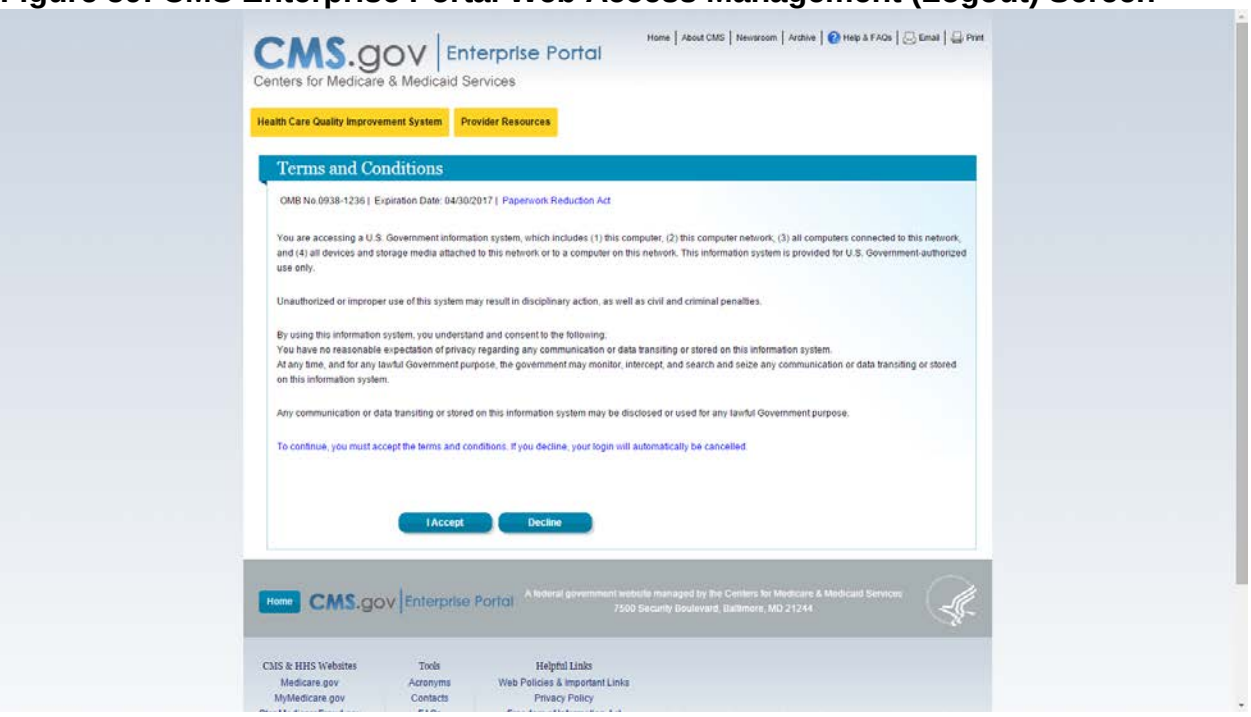
4.4. Application Organization & Navigation

Specific functionality and screen captures are described in Section 5.1 of this document.

4.5. Exiting the Application

Select the [Exit] link in the top right corner of any screen in the HPG Application to logout from the HPG application. You will be logged out of the HPG application and redirected to the ***CMS Enterprise Portal Web Access Management (Logout)*** screen as illustrated by Figure 59.

Figure 59: CMS Enterprise Portal Web Access Management (Logout) Screen



If you select [I Accept] you will be redirected to the ***Welcome to CMS Enterprise Portal login*** screen (Figure 55).

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 HPG application.

5.1. Application Layout

The application layout in the Site Map, as illustrated in Figure 60, is outlined as follows:

The links to navigate through the HPG application are:

- Home
- Submitter Profile
- NPI Management
- NPI Batch Management (available for Clearinghouse Submitters only)

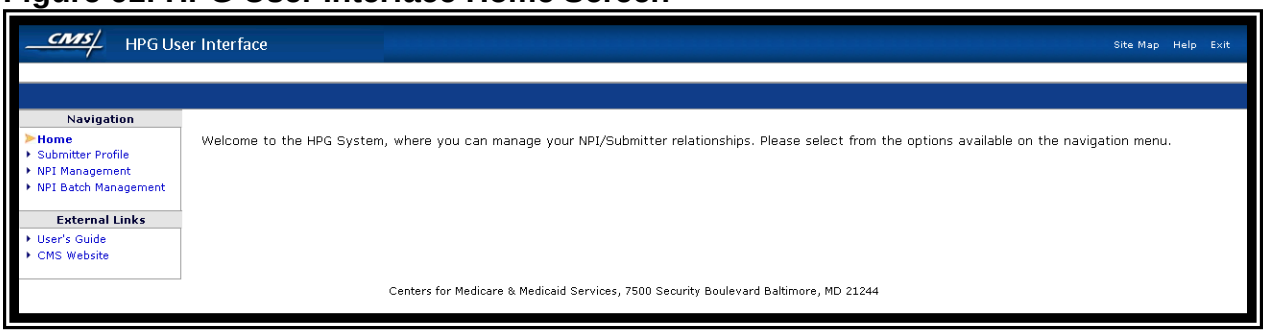
The links external to the HPG application are:

- User's Guide
- CMS Website

Figure 60: HPG Application Site Map

When you log into the HPG application, the ***HPG User Interface Home*** screen will display as illustrated in Figure 61.

Figure 61: HPG User Interface Home Screen



You are able to access the functionality of the HPG application by selecting the hyperlinks from the left-hand navigation bar. Additional hyperlinks are available in the top right of the screen. All hyperlinks are accessible and viewable on each screen in the HPG application.

The top right-hand hyperlinks are:

- Site Map – Provides the design layout of the HPG application.
- Help – Provides the MCARE Help Desk contact information.
- Exit – Closes the active HPG application session and redirects the User to the ***CMS Enterprise Portal Web Access Management (Logout)*** screen as illustrated in Figure 59.

The left-hand navigation hyperlinks are:

- Home – The HPG User Interface home page.
- Submitter Profile – Provides a list of active, valid Submitter IDs associated with the Submitter. This link is available to Clearinghouse and Direct Provider Submitters.

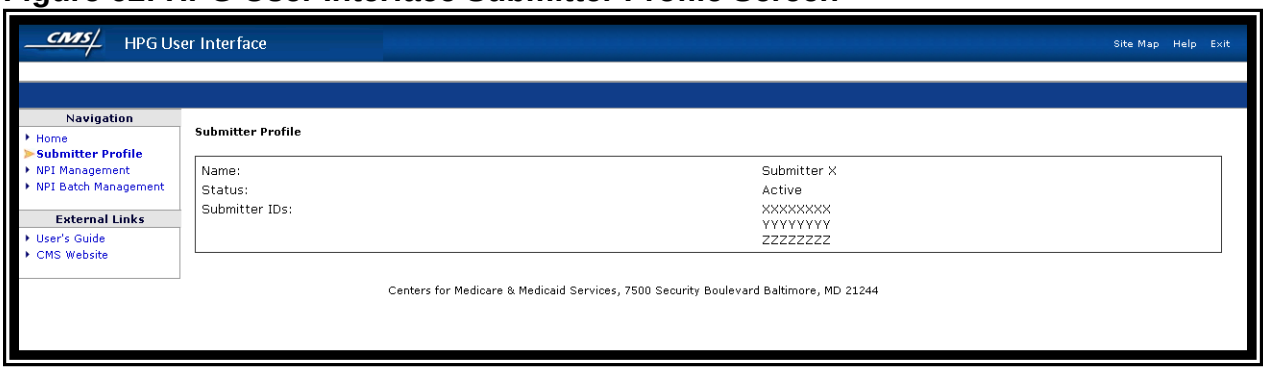
- NPI Management – Allows Submitters to add, terminate and/or query NPI numbers one at a time. This link is available to Clearinghouse and Direct Provider Submitters.
- NPI Batch Management – Provides a link to the Enterprise File Transfer (EFT) system. This link is available only to Clearinghouse Submitters.
- External Links – Provides links to the HPG User Guide and CMS Website.

5.2. Submitter Profile

The ***HPG User Interface Submitter Profile*** screen provides information regarding the Submitter's name, status, and active, valid Submitter ID(s). This is a view-only page that is available to Clearinghouse and Direct Provider Submitters.

To access your Submitter Profile, select the [Submitter Profile] link in the left-hand navigation menu. The ***HPG User Interface Submitter Profile*** screen will display as illustrated in Figure 62.

Figure 62: HPG User Interface Submitter Profile Screen

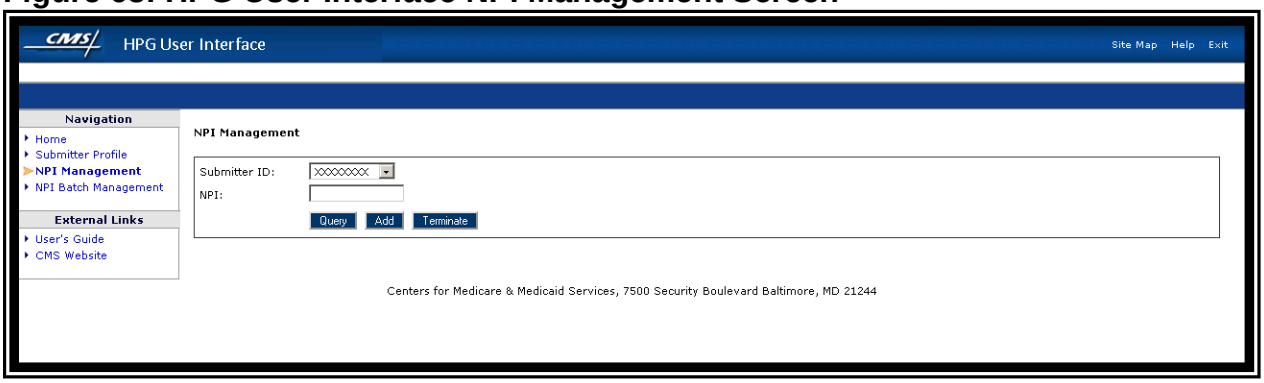


5.3. NPI Management

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

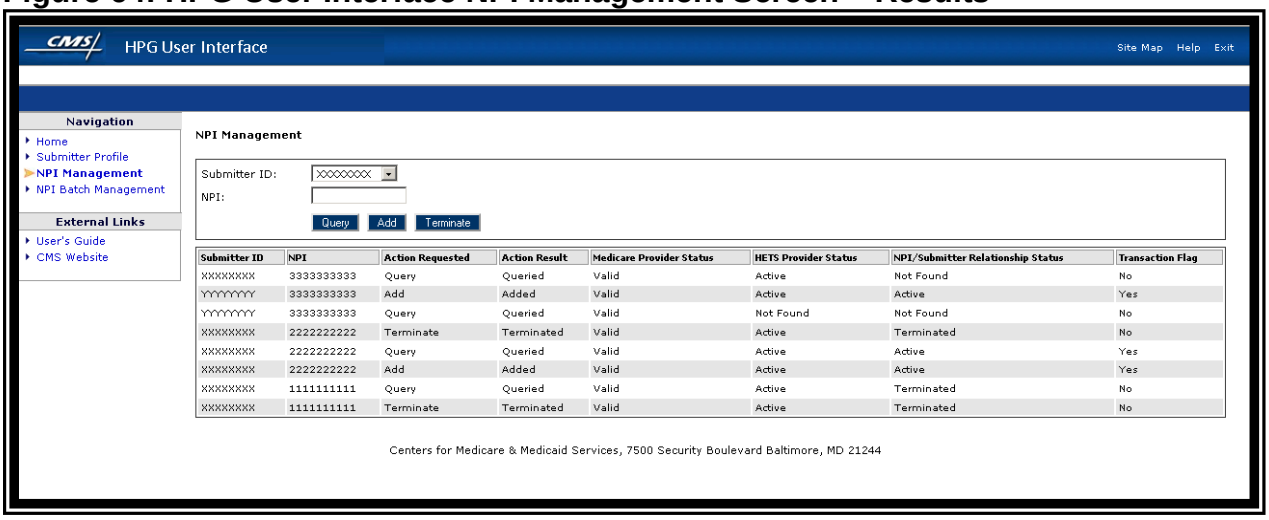
To access the NPI Management feature, select the [NPI Management] link in the left-hand navigation menu. The ***HPG User Interface NPI Management*** screen will display as illustrated in Figure 63.

Figure 63: HPG User Interface NPI Management Screen



Results for requested actions are displayed in an NPI Results table as illustrated in Figure 64.

Figure 64: HPG User Interface NPI Management Screen – Results



Submitter ID	NPI	Action Requested	Action Result	Medicare Provider Status	HETS Provider Status	NPI/Submitter Relationship Status	Transaction Flag
XXXXXXXX	3333333333	Query	Queried	Valid	Active	Not Found	No
XXXXXXXX	3333333333	Add	Added	Valid	Active	Active	Yes
XXXXXXXX	3333333333	Query	Queried	Valid	Not Found	Not Found	No
XXXXXXXX	2222222222	Terminate	Terminated	Valid	Active	Terminated	No
XXXXXXXX	2222222222	Query	Queried	Valid	Active	Active	Yes
XXXXXXXX	2222222222	Add	Added	Valid	Active	Active	Yes
XXXXXXXX	1111111111	Query	Queried	Valid	Active	Terminated	No
XXXXXXXX	1111111111	Terminate	Terminated	Valid	Active	Terminated	No

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 HPG based on the action selected by the User. Values include:
    - Queried – the query request has been processed by the HPG application and the query results are displayed in the NPI results table.

    - Added – the NPI/Submitter relationship has been added to the HPG 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 HPG 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.
- 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.
- 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 HPG application will display up to 25 rows in the NPI Results table. If more than 25 actions are performed during a single HPG application session, then the older results will no longer be displayed.

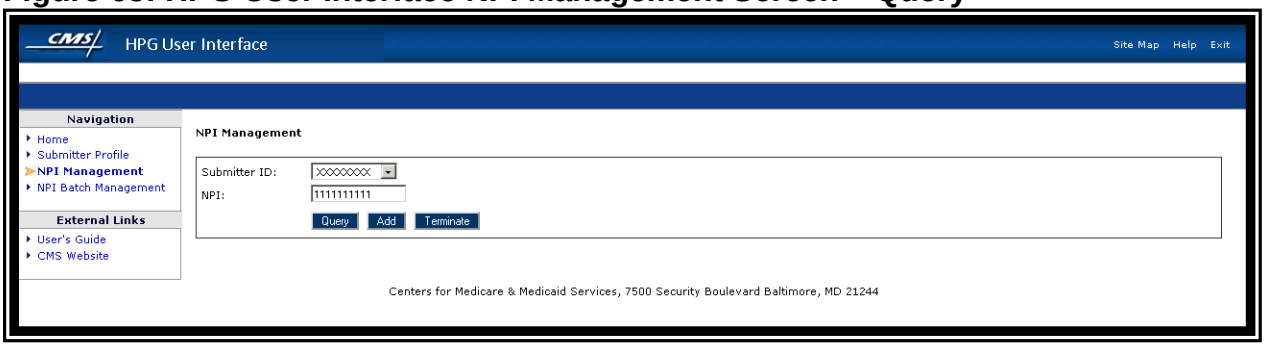
5.3.1. Query

5.3.1.1. 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 ***HPG User Interface NPI Management*** screen as illustrated in Figure 65:

Figure 65: HPG User Interface NPI Management Screen – Query



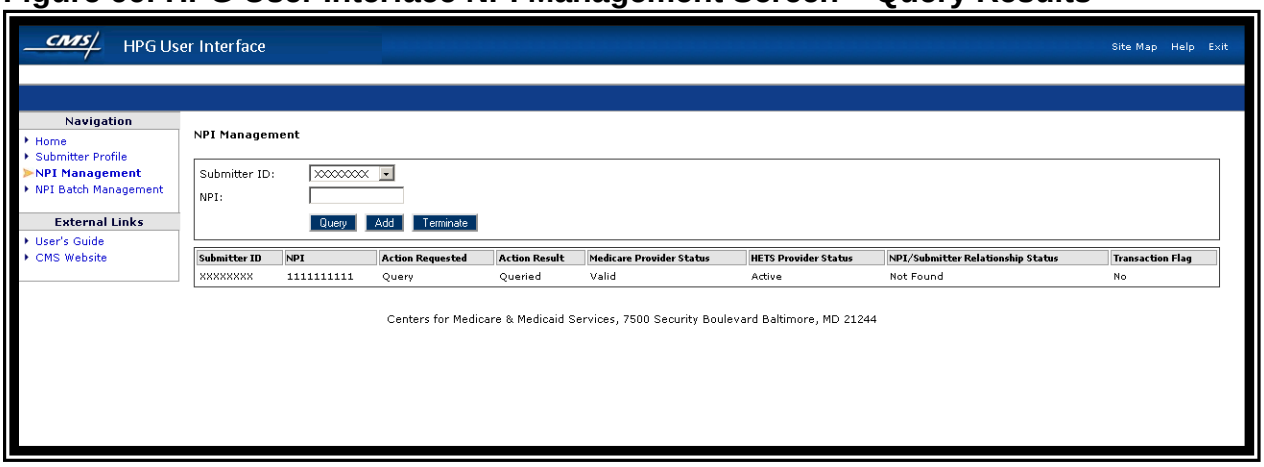
1. Select a Submitter ID from the drop-down list labeled Submitter ID.
2. Enter a 10-digit NPI number in the **NPI** field.
3. Select [Query].

   Note: The HPG 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.

5.3.1.2. Result

Figure 66 displays the NPI Results table for the query action.

Figure 66: HPG User Interface NPI Management Screen – Query Results



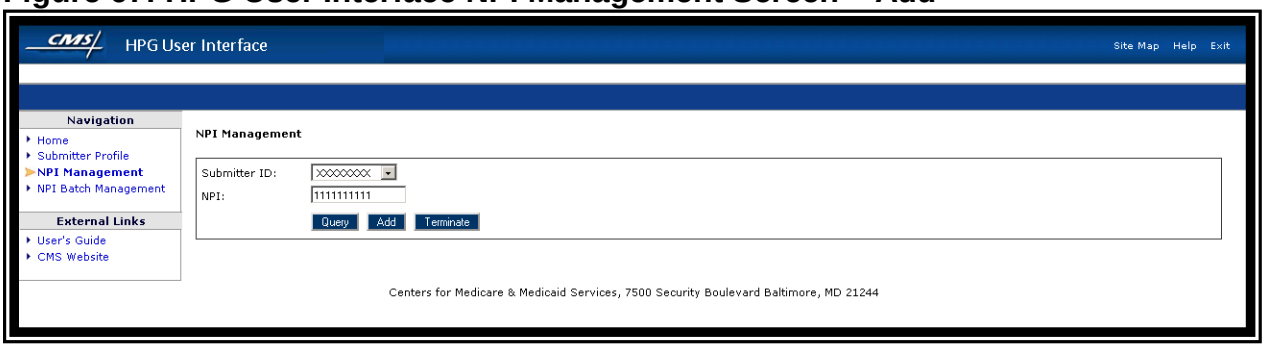
5.3.2. Add

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.

5.3.2.1. Action

To perform the add action; follow these steps on the ***HPG User Interface NPI Management*** screen as illustrated in Figure 67:

Figure 67: HPG User Interface NPI Management Screen – Add



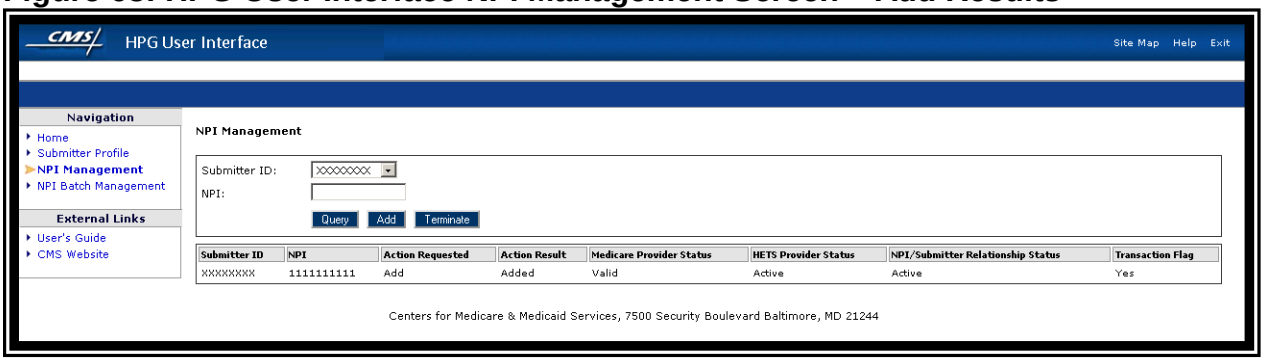
1. Select a Submitter ID from the selection box labeled Submitter ID.
2. Enter a 10-digit NPI number in the **NPI** field.
3. Select [Add].

   Note: The HPG 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.

5.3.2.2. Result

Figure 68 displays the NPI Results table for the add action.

Figure 68: HPG User Interface NPI Management Screen – Add Results



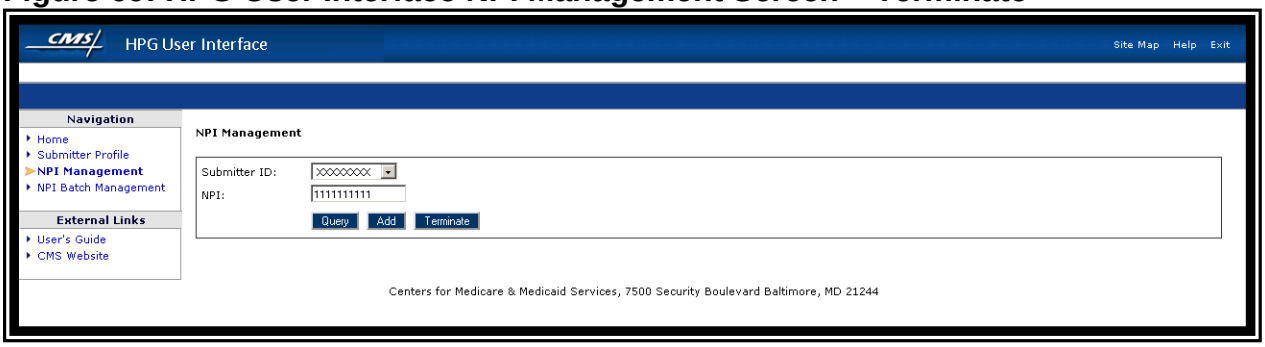
5.3.3. Terminate

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.

5.3.3.1. Action

To perform the terminate action; follow these steps on the ***HPG User Interface NPI Management*** screen as illustrated in Figure 69:

Figure 69: HPG User Interface NPI Management Screen – Terminate



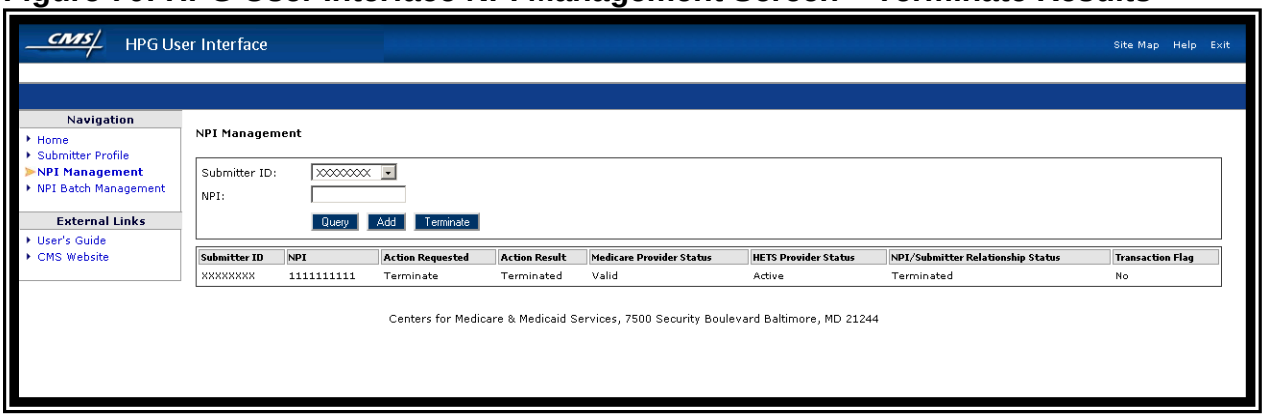
1. Select a Submitter ID from the selection box labeled Submitter ID.
2. Enter a 10-digit NPI number in the **NPI** field.
3. Select [Terminate].

   Note: The HPG 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.

5.3.3.2. Result

Figure 70 displays the NPI Results table for the terminate action.

Figure 70: HPG User Interface NPI Management Screen – Terminate Results



5.4. 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.

5.4.1. 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 71. The HPG application remains open in the background. Select [OK].

Figure 71: EFT Security Warning

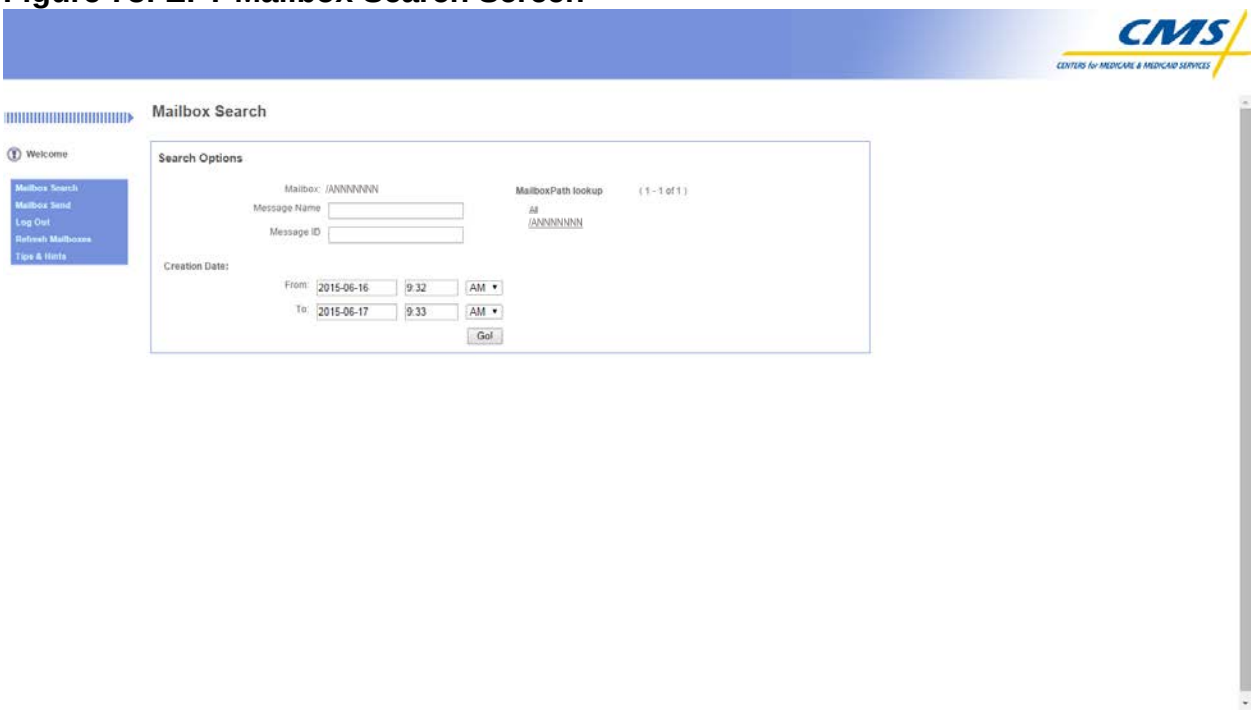
The ***Enterprise File Transfer Login*** screen now appears as illustrated in Figure 72.

Figure 72: 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 73.

Figure 73: EFT Mailbox Search Screen

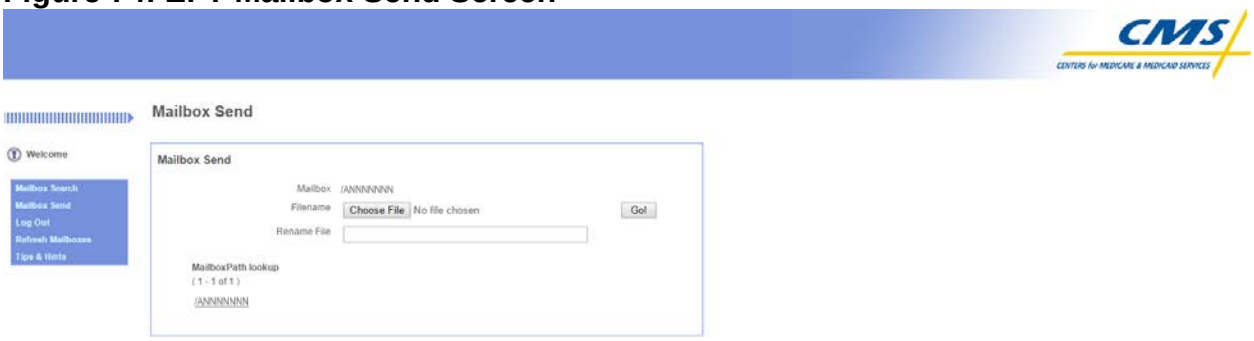


5.4.2. Uploading a File

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 73, select the Mailbox Send hyperlink in the left hand navigation menu. The ***EFT Mailbox Send*** screen will display as illustrated by Figure 74.

Figure 74: 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.HPG.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: T0000002)

   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 73.

5.4.3. 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 73. 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 75.

Figure 75: EFT Mailbox Search Results Screen

The naming convention for the results file(s) is:
P.HPGOUT.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

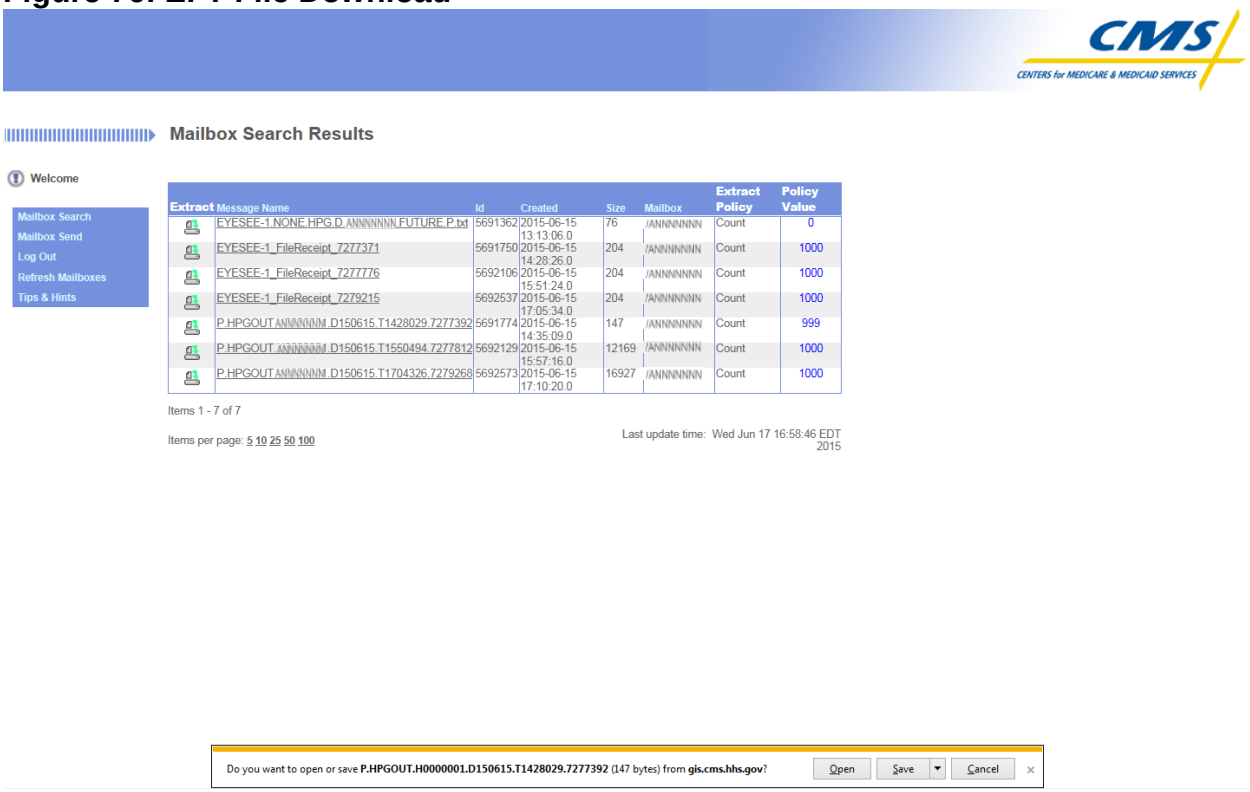
pn = Processing number assigned by EFT

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 76.

Figure 76: 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.

5.5. File Formats

5.5.1. 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.HPG.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

5.5.2. Output File

The output file generated by the HPG 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 or NE	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 HPG 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 HPG 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.

Data Element	Data Type	Possible Values	Description
Submitter Status	Alpha	A, S or T	The status of the Submitter in the HPG 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 or NF	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.
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.HPGOUT.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 HPG application.

6. TROUBLESHOOTING & SUPPORT

6.1. Troubleshooting

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

The HPG 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 HPG 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 HPG 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

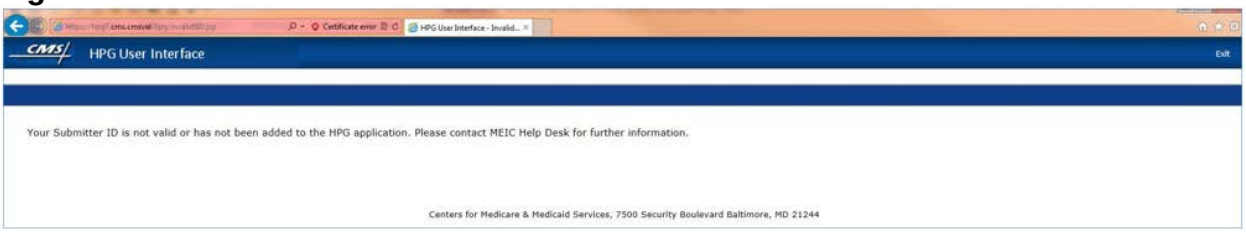
If you experience any problems while using the HPG application, contact the MCARE Help Desk. For contact information for the MCARE Help Desk, refer to Section 6.5.

6.3. Error Messages

6.3.1. Unauthorized Access

If you are not authorized to access the HPG application, the ***Unauthorized Access*** screen will display as illustrated in Figure 77.

Figure 77: Unauthorized Access Screen

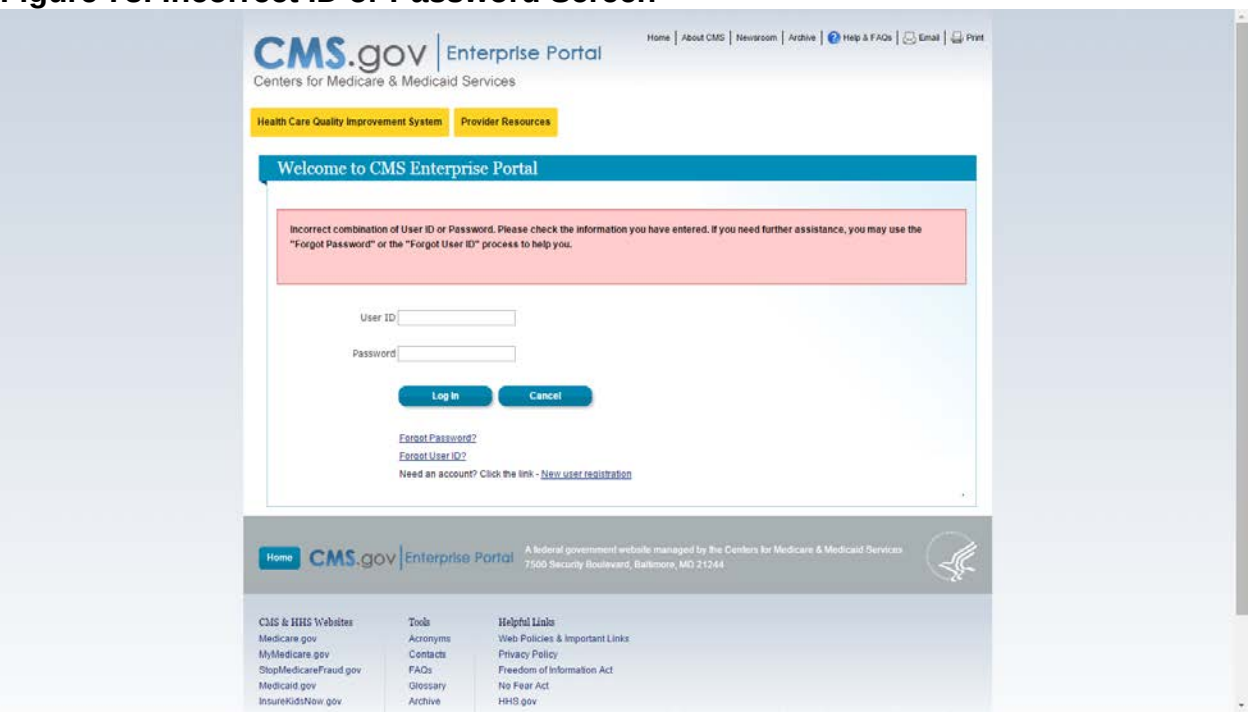


Contact the MCARE Help Desk for assistance if you think that you have received this message in error. For contact information for the MCARE Help Desk, refer to Section 6.5.

6.3.2. CMS Enterprise Portal Login

If you enter an incorrect/invalid CMS Enterprise Portal User ID or password, the ***Incorrect ID or Password*** screen will display the message as illustrated in Figure 78.

Figure 78: Incorrect ID or Password Screen



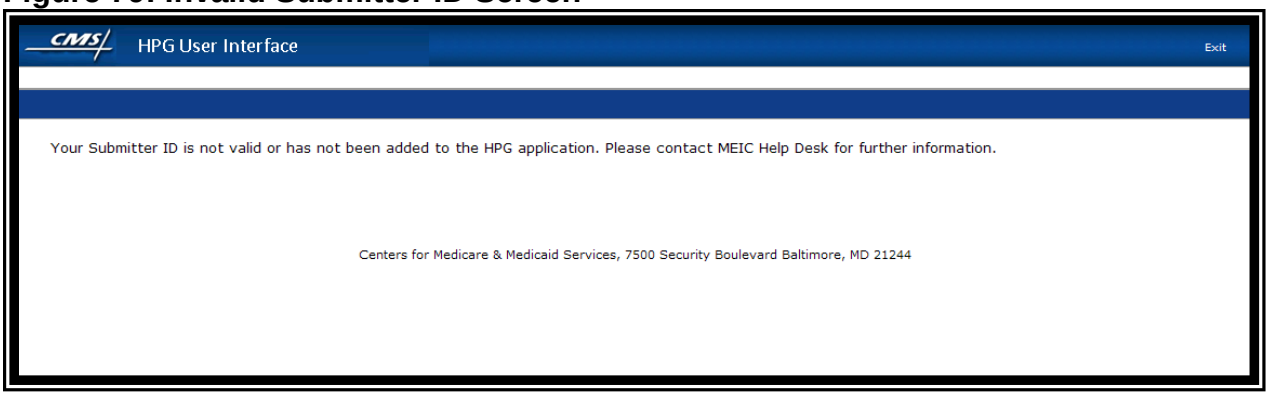
Enter a valid CMS Enterprise Portal User ID in the **User ID** field. Enter a valid CMS Enterprise Portal password in the **Password** field. Select [Log In].

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. Invalid Submitter ID

If you login to HPG with a valid CMS Enterprise Portal User ID and password, but the Submitter ID in your CMS Enterprise Portal profile is missing or invalid, the ***Invalid Submitter ID*** screen will display the message as illustrated in Figure 79.

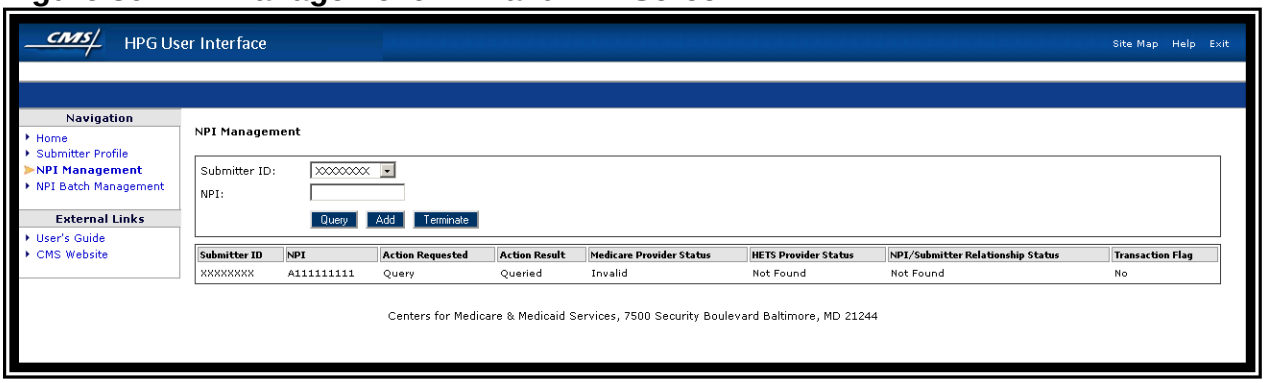
Figure 79: Invalid Submitter ID Screen



6.3.4. Missing or Invalid NPI

On the ***NPI Management*** 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 80 for an illustration.

Figure 80: NPI Management – Invalid NPI Screen



6.3.5. Batch File Error Messages

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

Table 5: Batch File Error Messages

Error Message	Condition(s)
Failed to validate file. The file is empty.	The batch file contains no data.
Line #${lineNumber}: Each line must have 3 values: Submitter ID, NPI, and Action	A line in the batch file does not include the 3 requisite elements.
Line #${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 HPG.

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 HPG application; however, the EFT file transfer system has a file size limitation of 1GB.

6.4.2. Daily Batch File Submission

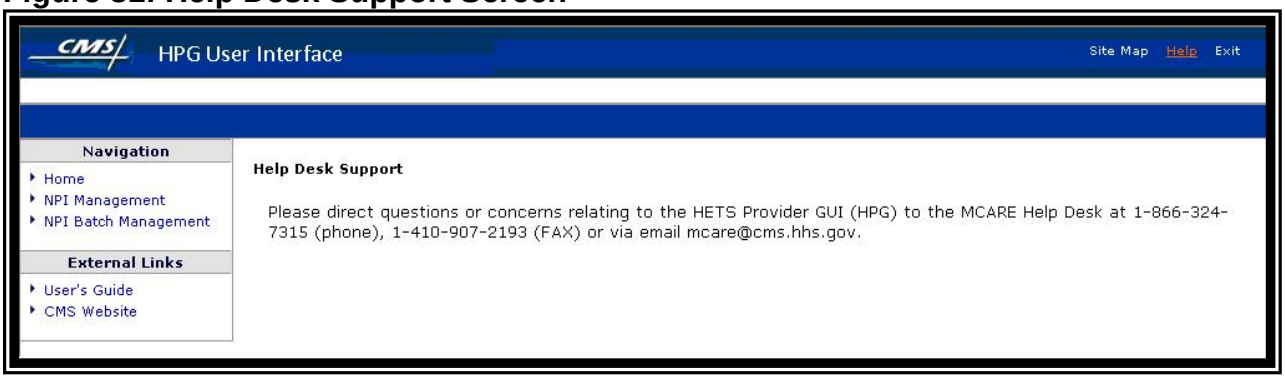
Clearinghouse Submitters are limited to uploading only one batch file per day. If a Clearinghouse Submitter attempts to upload more than one file during a single calendar day, an error message will be returned in the batch output file.

6.5. System Support Information

If problems and/or questions arise while accessing the HPG 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.

The Help link within the HPG application, as illustrated in Figure 81, also provides the contact information for the MCARE Help Desk.

Figure 81: Help Desk Support Screen



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.

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 HPG application.

8. ACRONYMS

Table 6 identifies acronyms and definitions used in this document.

Table 6: 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
HETS	HIPAA Eligibility Transaction System
HPG	HETS Provider Graphical User Interface
MCARE	Medicare Customer Assistance Regarding Eligibility
MFA	Multi-Factor Authentication
NPI	National Provider Identifier
PHI	Protected Health Information
RIDP	Remote Identity Proofing