



Office of Hearings Case and Document Management System (“OH CDMS”)

External Registration and User Access Manual

Version 1.0
July 10, 2018



Table of Contents

List of Figures	iii
List of Tables	v
1. Introduction	1
1.1 Office of Hearings Case and Document Management System	1
1.2 CMS Enterprise Portal.....	1
1.3 Cautions & Warnings.....	1
1.3.1 Identity Verification.....	1
1.3.2 Multi-Factor Authentication	2
1.3.3 Session Timeout	2
1.3.4 Password Timeframes	2
1.3.5 Annual Certification.....	2
1.4 Accessibility Standards.....	2
2. Getting Started.....	3
2.1 Set-up Considerations	3
2.2 User Access Considerations.....	3
3. Access the CMS Enterprise Portal Public Landing Page	4
4. Register for Secure CMS Enterprise Portal Access.....	6
4.1 Step #1: Choose Your Application	6
4.2 Step #2: Register Your Information.....	8
4.3 Step #3: Create User ID, Password & Challenge Questions.....	9
4.4 Registration Summary and Confirmation	11
5. Request Access to Salesforce.....	12
5.1 Request/Add Apps.....	12
5.2 Identity Verification	15
5.3 Multi-Factor Authentication	19
5.4 Complete Access Request	22
6. Access the Salesforce App Store.....	25

7. Request OH CDMS User Role 31

8. Launch OH CDMS 34

9. Support 38

 9.1 OH CDMS Helpdesk.....38

 9.2 CMS Enterprise Portal Reference Materials38

Appendix A: Acronyms..... 39

Appendix B: Record of Changes 40

List of Figures

Figure 1: CMS Enterprise Portal Public Landing Page	4
Figure 2: CMS Enterprise Portal Header	5
Figure 3: CMS Enterprise Portal Landing Page – New User Registration Button	6
Figure 4: Choose Your Application Page.....	6
Figure 5: Choose Your Application – Salesforce Option in Drop-Down List.....	7
Figure 6: Choose Your Application – Terms & Conditions Agreement.....	7
Figure 7: Register Your Information Page	8
Figure 8: Create User ID, Password & Challenge Questions Page	9
Figure 9: User ID Field with Requirements Tool Tip	9
Figure 10: Password Field with Requirements Tool Tip.....	10
Figure 11: Challenge Question and Answer Fields.....	10
Figure 12: New User Registration Confirmation	11
Figure 13: Initial Login Screen.....	12
Figure 14: My Portal Page – Accessing the Application Catalog	12
Figure 15: Access Catalog	13
Figure 16: Access Catalog – Filter Field.....	13
Figure 17: Access Catalog – Salesforce Application Tile with Request Access Button.....	14
Figure 18: Request New Application Access – Application Description and Help Window	14
Figure 19: Request New Application Access – Select a Role Drop-Down	14
Figure 20: Request New Application Access – Salesforce User Selection	14
Figure 21: Identity Verification Information	15
Figure 22: Terms & Conditions.....	15
Figure 23: Agree to Terms & Conditions	16
Figure 24: Your Information Page (Part 1).....	16
Figure 25: Your Information Page (Part 2).....	17
Figure 26: Your Information – Sample Tool Tip.....	17
Figure 27: Your Information – Sample Error Messages.....	18
Figure 28: Verify Identity Page	18
Figure 29: Multi-Factor Authentication Information Page.....	19
Figure 30: Register Phone, Computer, or Email for MFA Access	20
Figure 31: MFA Device Type Drop-Down Menu	20
Figure 32: VIP Access Display	21
Figure 33: MFA Registration Fields – Phone/Tablet/PC/Laptop	21

Figure 34: MFA Registration Confirmation	22
Figure 35: Update Profile Page	22
Figure 36: Reason for Request	23
Figure 37: Review Request.....	23
Figure 38: Request New Application Access Acknowledgement	24
Figure 39: Portal Login Page.....	25
Figure 40: Choose MFA Device Drop-Down Menu.....	25
Figure 41: MFA Device Options	26
Figure 42: Selecting Tablet/PC/Laptop Option as MFA Device	26
Figure 43: Selecting Text Message (SMS) as MFA Device	26
Figure 44: Selecting Interactive Voice Response as MFA Device	27
Figure 45: Selecting Email as MFA Device	27
Figure 46: My Portal.....	27
Figure 47: My Portal – Salesforce Application	27
Figure 48: CMS App Launcher	28
Figure 49: CMS App Store	28
Figure 50: CMS App Store – Filtered for OH	28
Figure 51: CMS App Store – OH CDMS Application Tile.....	29
Figure 52: CMS App Listing – OH CDMS Application.....	29
Figure 53: Request Details Window	30
Figure 54: Application Request Confirmation	30
Figure 55: Community Registration Page.....	31
Figure 56: Requester Organization Type Drop-Down Menu	32
Figure 57: Hearing Officer Petitioner Type Drop-Down Menu.....	32
Figure 58: Organization Information Page.....	32
Figure 59: Community Registration Page – New Organization Fields	33
Figure 60: Application Request Conformation	33
Figure 61: Login Page.....	34
Figure 62: My Portal.....	34
Figure 63: CMS App Launcher	35
Figure 64: OH CDMS Community Rules of Behavior	36
Figure 65: OH CDMS Landing Page	37

List of Tables

Table 1: Acronyms	39
Table 2: Record of Changes	40

1. Introduction

This user manual provides step-by-step instructions for new external users requesting access to the Office of Hearings Case and Document Management System ("OH CDMS") application through the Centers of Medicare & Medicaid Services ("CMS") Enterprise Portal.

1.1 Office of Hearings Case and Document Management System

The Office of Hearings Case and Document Management System is a web-based portal for parties to enter and maintain their cases and to correspond with the Office of Hearings ("OH"). OH supports three distinct administrative hearing functions:

- The **Provider Reimbursement Review Board** ("PRRB"): provider appeals of cost report audits and other final determinations per 42 C.F.R. § 405, Subpart R;
- The **Medicare Geographic Classification Review Board** ("MGCRB"): hospital applications to request geographic redesignation to an alternative payment area per 42 C.F.R. § 412, Subpart L; and
- The **CMS Hearing Officer**: diverse range of matters brought by healthcare institutions, insurance issuers, state Medicaid plans, organ procurement organizations, and other entities per various regulatory authorities.

Access to the various modules is granted as needed based on role. Access to specific cases is limited to the parties of each case and their representatives.

1.2 CMS Enterprise Portal

The CMS Enterprise Portal is a single point of entry to numerous CMS applications and systems. The portal supports users' role-based access and personalization to present each user with only relevant content and applications (e.g., OH CDMS, which is housed within the Salesforce Application). Registration is a multi-step process to obtain secure access to both the portal itself and to the specific application.

1.3 Cautions & Warnings

1.3.1 Identity Verification

Users are required to enter some personal information and choose a desired User ID and Password following the guidelines provided to login to the CMS Enterprise Portal. Users are further provisioned by the Enterprise Identity Management ("EIDM") mechanism for identity verification. CMS uses [Experian](#) as the external authentication service provider.

The identity verification process involves Experian using information from your credit report solely to help confirm your identity in order to avoid fraudulent access or transactions in your name. As a result, you may see an entry called a "soft inquiry" on your Experian credit report. Soft inquiries do not affect your credit score and do not incur any charges related to them. You may need access to your personal and credit report information as the Experian application will pose questions to you based on historical data in Experian's files. For additional information, please see the Experian Consumer Assistance website at <http://www.experian.com/help/>.

1.3.2 Multi-Factor Authentication

Multi-Factor Authentication (“MFA”) is a security mechanism that is implemented to provide an extra layer of security, through the use of a unique security code, in addition to the entry of a User ID and Password. Since OH CDMS is a MFA-protected application, the CMS EIDM system requires registration of a phone or computer as a means to obtain the necessary security code.

To complete the MFA registration process, users are given four options from which to select:

1. Phone/Tablet/PC/Laptop via the Validation & ID Protection (“VIP”) Access Software; 2. Text Message Short Message Service (“SMS”); 3. Interactive Voice Response (“IVR”); and 4. Email. At each login, users will be prompted to obtain a current security code from the registered MFA device.

While the security code for the VIP Access Software refreshes automatically every 30 seconds, the security code for the SMS and IVR options expires in 10 minutes, and the security code for the email option expires in 30 minutes. If you are unable to enter the code within the allotted period, you must request a new one.

1.3.3 Session Timeout

Session timeout occurs if users do not perform any action on the CMS Enterprise Portal site and remain inactive for 30 minutes. When this happens, a session pop-up message is displayed to the users allowing them to either stay logged in or log out from the system. If neither option is selected by the user within 2 minutes, the session will automatically be terminated.

1.3.4 Password Timeframes

Your password must be changed at least every 60 days to remain an active user within the CMS Enterprise Portal and its associated systems and applications. Passwords can be changed only once every 24 hours.

1.3.5 Annual Certification

CMS security guidelines require an annual certification of a user’s role. Annual Certification is typically performed in the same manner as the original role approval process used by Business Owners, their representatives, authorizers, Help Desks, or other approvers. If the continued use of a role is not approved, then the role will be removed from your profile.

1.4 Accessibility Standards

CMS is committed to making its electronic and information technologies accessible to people with disabilities. We strive to meet or exceed the requirements of Section 508 of the Rehabilitation Act (29 U.S.C. § 794d), as amended in 1998.

If any content or use of any features in the CMS Enterprise Portal cannot be accessed due to a disability, please contact our Section 508 Team via email at 508Feedback@cms.hhs.gov.

For more information on CMS Accessibility and Compliance with Section 508, see the [CMS Accessibility & Nondiscrimination for Individuals with Disabilities Notice](#).

2. Getting Started

2.1 Set-up Considerations

CMS screens are designed to be viewed at a minimum screen resolution of 1024 x 768. For optimal performance, screen resolution should be set to 1920 x 1080. The following additional considerations optimize access to CMS Enterprise Portal:

- Disable pop-up blockers prior to accessing CMS Enterprise Portal.
- Use one of the following browsers with JavaScript enabled:
 - Internet Explorer (IE), version 11.0 or higher;
 - Chrome (recommended for optimal performance);
 - Firefox; or
 - Safari.

2.2 User Access Considerations

Six distinct steps are required to obtain access to OH CDMS:

- Access the CMS Enterprise Portal public landing page.
- Register for secure CMS Enterprise Portal access.
- Request access to Salesforce.
- Access Salesforce App Store.
- Request OH CDMS user role.
- Launch OH CDMS.

3. Access the CMS Enterprise Portal Public Landing Page

Navigate to the CMS Enterprise Portal at <https://portal.cms.gov>. The CMS Enterprise Portal public landing page is displayed.

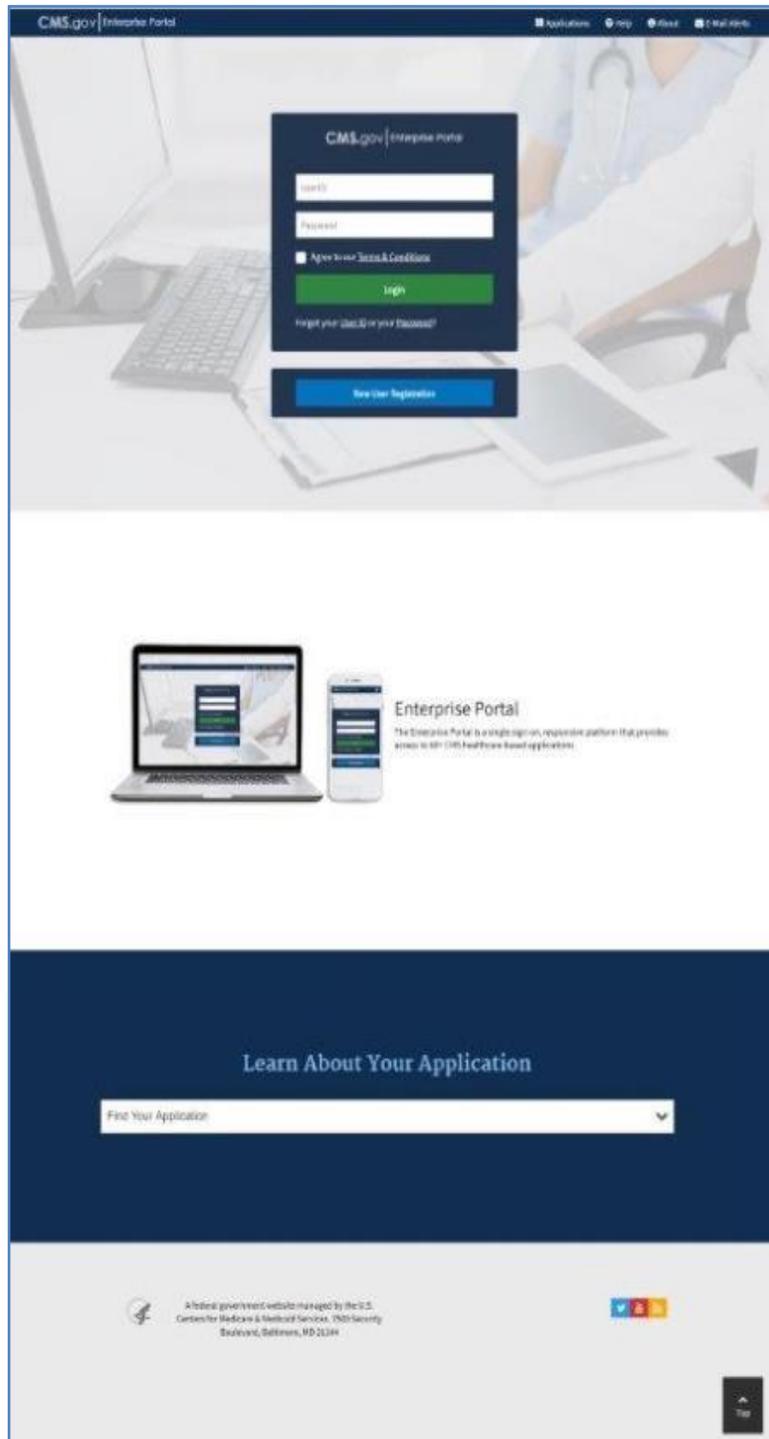


Figure 1: CMS Enterprise Portal Public Landing Page

The header is designed with the following navigation elements:

- ***CMS.gov/Enterprise Portal link:*** Clicking this link performs a page refresh of the landing page.
- ***Applications:*** Clicking this link allows users to select their application from a drop-down menu and view their application's helpdesk and support information.
- ***Help link:*** Clicking this link redirects users to a help page containing general help information.
- ***About link:*** Clicking this link displays information about CMS.
- ***E-Mail Alerts link:*** CMS Enterprise Portal email alerts is a communication tool that allows Portal users to subscribe to notification lists which deliver important and timely CMS information. Users can elect to receive CMS Enterprise Portal email alerts by clicking the E-Mail Alerts link.



Figure 2: CMS Enterprise Portal Header

4. Register for Secure CMS Enterprise Portal Access

On the CMS Enterprise Portal landing page, click the **New User Registration** button.

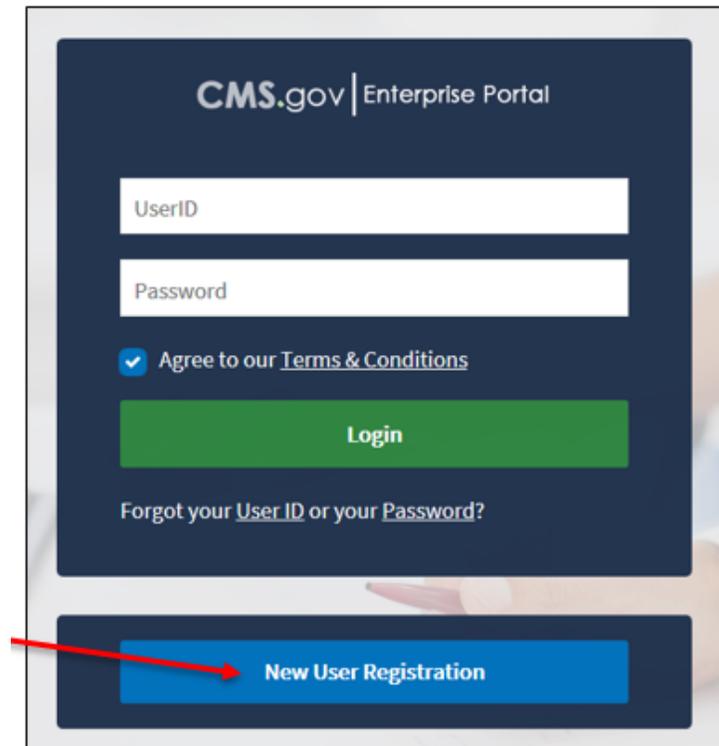


Figure 3: CMS Enterprise Portal Landing Page – New User Registration Button

4.1 Step #1: Choose Your Application

The **Choose Your Application** page contains a drop-down menu with a variety of CMS applications available to select.

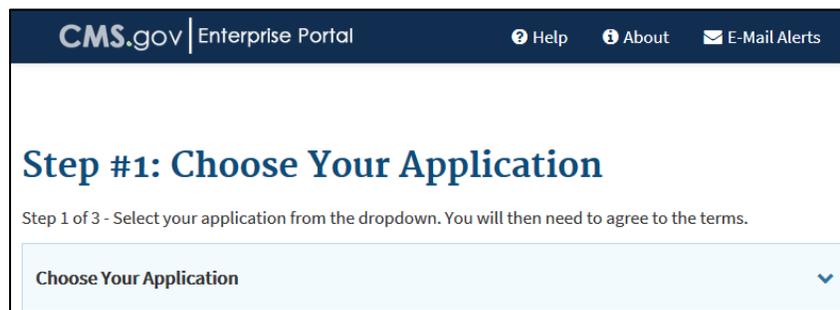


Figure 4: Choose Your Application Page

1. From the drop-down list, select the **Salesforce** application. Salesforce is the cloud-based platform on which OH CDMS is built.

Step #1: Choose Your Application

Step 1 of 3 - Select your application from the dropdown. You will then need to agree to the terms.

Choose Your Application

- Open Payments: Physician Payments Sunshine Act
- PECOS AI: Provider Enrollment, Chain & Ownership System
- PECOS Data Mart: Provider Enrollment, Chain & Ownership System Data Mart
- PMDA: Performance Metrics Database & Analytics
- PRIS: Payment Recovery Information System
- PQRS: Physician Quality Reporting System
- PSR/STAR: Provider Statistical and Reimbursement/System for Tracking Audit and Reimbursement
- PV: Physician Quality and Value Programs
- QARM: Quality Net Authorization & Role Management
- RNSGUI: Research and Support Graphical User Interface
- Salesforce**
- SERTS: State Exchange Resource Tracking System
- SERVIS: State Exchange Resource Virtual Information System
- SHIM: Enrollment and Payment Portal
- SPOT(FCSO): First Coast Service Options Internet Portal
- STARS: Services Tracking Analysis and Reporting System
- T-MSIS: Transformed Medicaid Statistical Information System
- UCM: Unified Case Management
- VMS Client Letter: VMS Durable Medical Equipment DME Client Letter Application
- zONE: Opportunity to Network and Engage

Figure 5: Choose Your Application – Salesforce Option in Drop-Down List

2. Review the Terms & Conditions information and indicate agreement by selecting the checkbox that states “**I agree to the terms and conditions.**” Select the **Next** button to continue with the registration process. The button is disabled until you select the checkbox.

Step #1: Choose Your Application

Step 1 of 3 - Select your application from the dropdown. You will then need to agree to the terms.

Salesforce

Terms & Conditions

OMB No.0938-1236 | Expiration Date: 03/31/2021 | [Paperwork Reduction Act](#)

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](#).

I agree to the terms and conditions

Next Cancel

Figure 6: Choose Your Application – Terms & Conditions Agreement

4.2 Step #2: Register Your Information

The **Register Your Information** page displays a number of fields to enter personal and contact information to complete the identity verification process.

1. Provide the information requested on the page. All fields are required and must be completed unless marked “Optional”.
2. After all required information has been completed, click the **Next** button to continue.
3. Note that you may click **Cancel** at any time to exit out of the registration process. If you cancel, then any changes entered will not be saved. To go to the previous step, click the **Back** button.

Step #2: Register Your Information

Step 2 of 3 - Please enter your personal and contact information.
All fields are required unless marked 'Optional'.

Enter First Name	Enter Middle Name (optional)	Enter Last Name	Suffix (optional)
Enter Social Security Number (optional)	Birth Month	Birth Date	Birth Year

Is Your Address US Based?

Yes No

Enter Home Address #1	Enter Home Address #2 (optional)		
Enter City	State	Enter Zip Code	Enter Zip+4 (optional)
Enter E-mail Address	Confirm E-mail Address		
Enter Phone Number			

Figure 7: Register Your Information Page

4.3 Step #3: Create User ID, Password & Challenge Questions

The **Create User ID, Password & Challenge Questions** page displays fields to create login information for future access to the Enterprise Portal.

Step #3: Create User ID, Password & Challenge Questions

Step 3 of 3 - Please create User ID and Password, Select Challenge questions and provide answers.

Enter User ID

Enter Password Enter Confirm Password

Select Challenge Question #1 Enter Challenge Question #1 Answer

Select Challenge Question #2 Enter Challenge Question #2 Answer

Select Challenge Question #3 Enter Challenge Question #3 Answer

Back Next Cancel

Figure 8: Create User ID, Password & Challenge Questions Page

1. Create and enter a user ID in the **Enter User ID** field based on the established user ID requirements. Instructions are displayed in the form of a tool tip window when selecting the field.

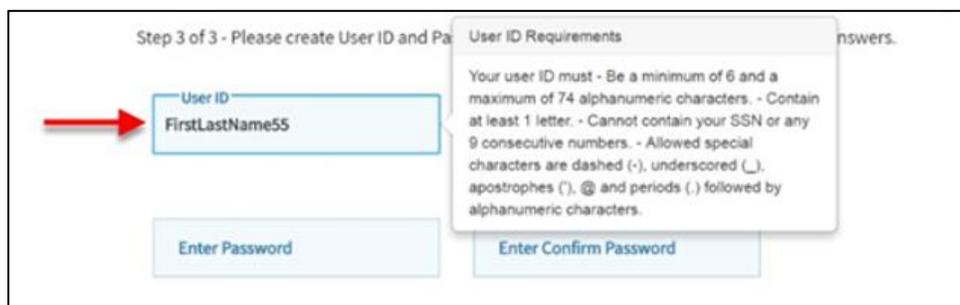


Figure 9: User ID Field with Requirements Tool Tip

2. Create and enter a password in the **Enter Password** field based on the established password requirements. Instructions are displayed in the form of a tool tip window when selecting the field. Enter the same password in the **Confirm Password** field.



Figure 10: Password Field with Requirements Tool Tip

3. After entering the user ID and password, select a question in the **Select Challenge Question #1** drop-down list and then enter the answer you want to be saved with the question.
4. Continue to select a question and enter an answer for Question #2 and Question #3. Click **Next** to complete the registration process.

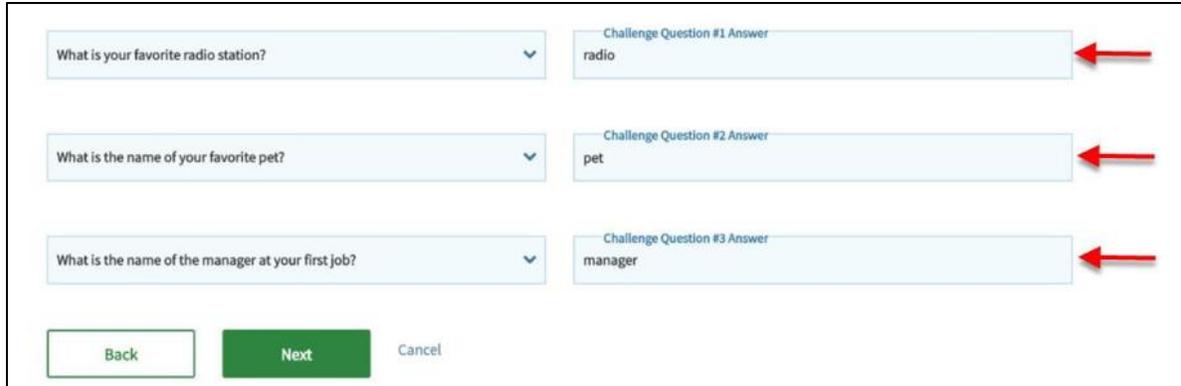
The screenshot shows three rows of challenge questions and answers. Each row consists of a question dropdown and an answer text field. The first row has the question "What is your favorite radio station?" and the answer "radio". The second row has the question "What is the name of your favorite pet?" and the answer "pet". The third row has the question "What is the name of the manager at your first job?" and the answer "manager". Red arrows point to the answer fields. At the bottom, there are three buttons: "Back", "Next" (highlighted in green), and "Cancel".

Figure 11: Challenge Question and Answer Fields

4.4 Registration Summary and Confirmation

The **Registration Summary** page displays all the previously entered information for confirmation. Review the information you entered, make any necessary changes and then click the **Submit User** button.

The **Confirmation** page is displayed acknowledging your successful registration and informs you that you will also receive a confirmation email to your registered email address.

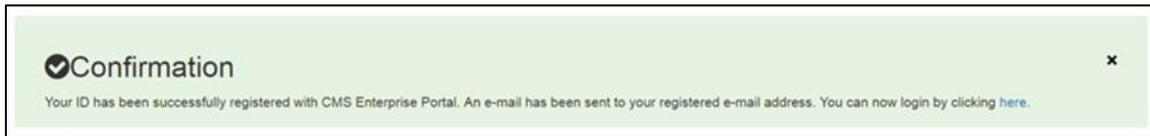


Figure 12: New User Registration Confirmation

5. Request Access to Salesforce

Users must have completed the registration process and have an active user ID and password credentials to request access to the Salesforce application and its associated roles.

1. Navigate to the CMS Enterprise Portal at <https://portal.cms.gov>.
2. Login using your user ID and password.

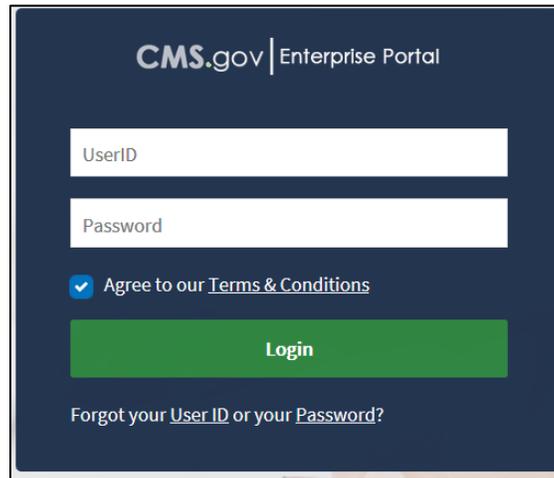


Figure 13: Initial Login Screen

5.1 Request/Add Apps

1. After logging in, the **My Portal** page is displayed. Select the **Request/Add Apps** tile or select the **My Access** option from the Welcome drop-down list in the top navigation bar to access the Application Catalog.

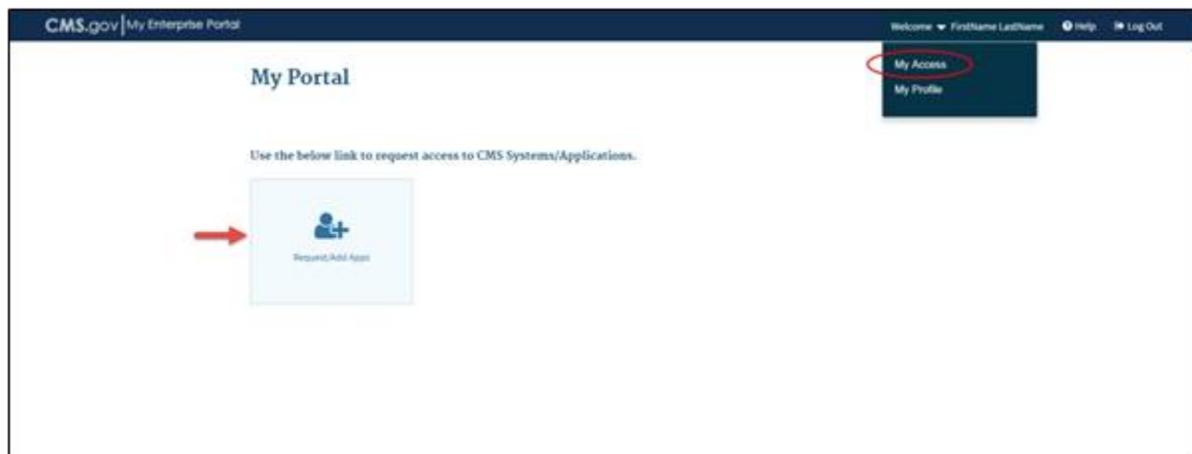


Figure 14: My Portal Page – Accessing the Application Catalog

- The **Access Catalog** page is displayed. The Access Catalog includes all the CMS applications that use EIDM services.

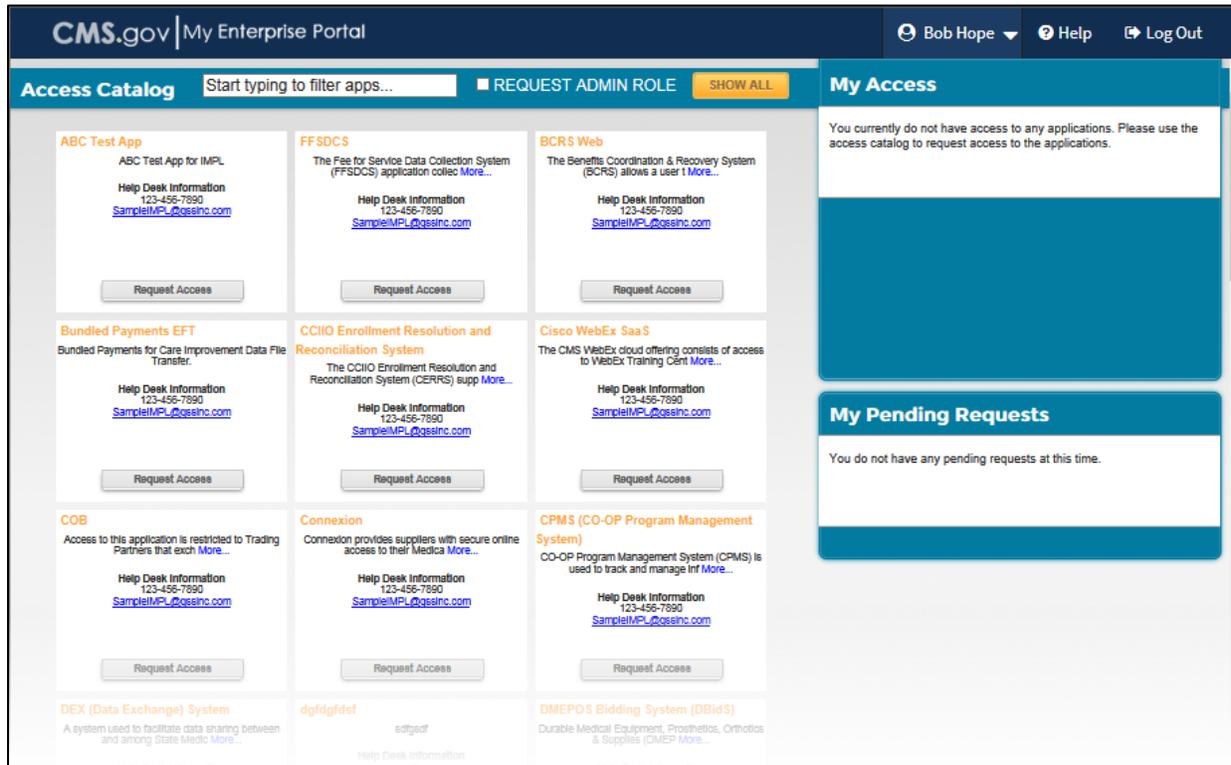


Figure 15: Access Catalog

- Type “salesforce” into the Access Catalog filter field and click Enter to search for the application tile that is specific to the Salesforce platform.

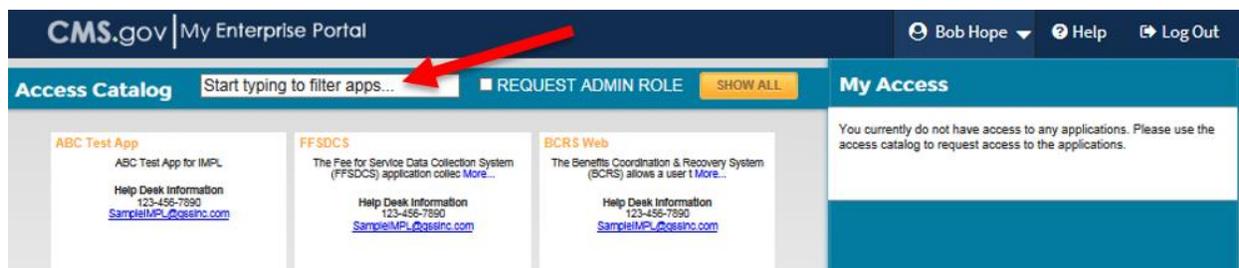


Figure 16: Access Catalog – Filter Field

4. The **Salesforce** tile is displayed. Select the **Request Access** button to continue.

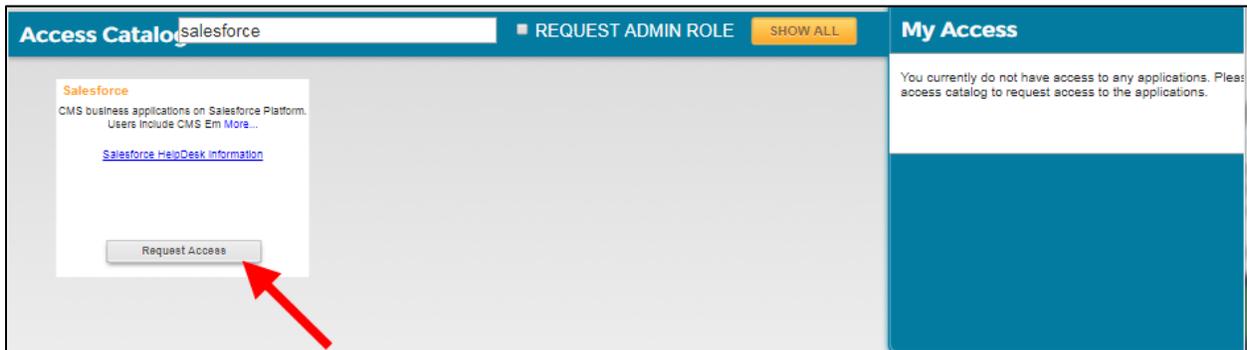


Figure 17: Access Catalog – Salesforce Application Tile with Request Access Button

5. The **Request New Application Access** page is displayed. Salesforce is pre-populated in the **Application Description** drop-down menu. There is an Interactive Help window on the right that will automatically update as you navigate through the site.

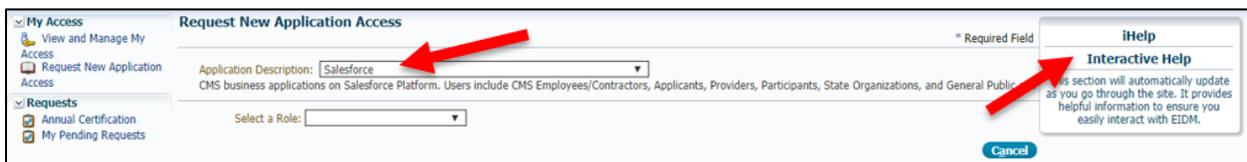


Figure 18: Request New Application Access – Application Description and Help Window

6. Select **Salesforce user** from the **Select a Role** drop-down menu.

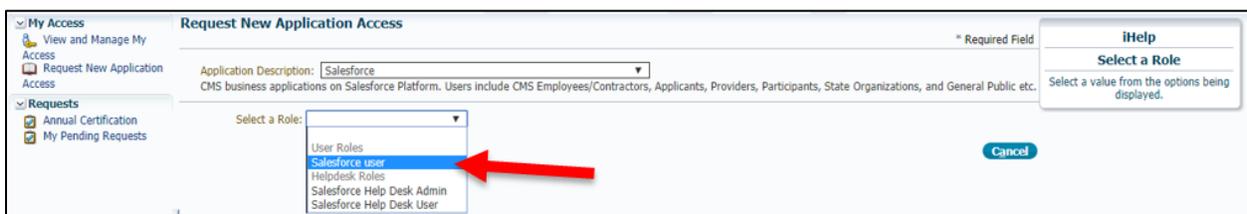


Figure 19: Request New Application Access – Select a Role Drop-Down

7. A role description is displayed along with a message indicating that this role requires identity verification. Select the **Next** button to continue.

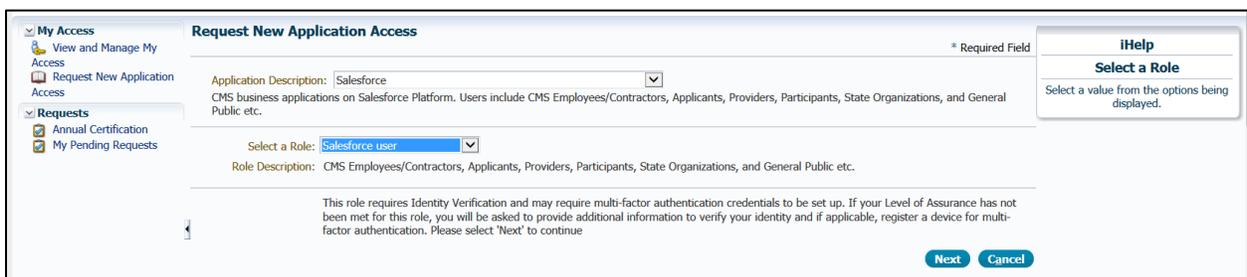


Figure 20: Request New Application Access – Salesforce User Selection

5.2 Identity Verification

1. The **Identity Verification** information page is displayed. Read the information and select **Next** to continue.

Request New Application Access

Identity Verification

To protect your privacy, you will need to complete Identity Verification successfully, before requesting access to the selected role. Below are a few items to keep in mind.

- Ensure that you have entered your legal name, current home address, primary phone number, date of birth and email address correctly. We will only collect personal information to verify your identity with Experian, an external Identity Verification provider.
- Identity Verification involves Experian using information from your credit report to help confirm your identity. As a result, you may see an entry called a "soft inquiry" on your Experian credit report. Soft inquiries do not affect your credit score and you do not incur any charges related to them.
- You may need to have access to your personal and credit report information, as the Experian application will pose questions to you, based on data in their files. For additional information, please see the Experian Consumer Assistance website - <http://www.experian.com/help/>

If you elect to proceed now, you will be prompted with a Terms and Conditions statement that explains how your Personal Identifiable Information (PII) is used to confirm your identity. To continue this process, select 'Next'.

Next
Cancel

Figure 21: Identity Verification Information

2. The **Terms and Conditions** page is displayed. Review the information.

Terms and Conditions

OMB No. 0938-1236 | Expiration Date: 04/30/2017 (OMB Re-Certification Pending) | [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.

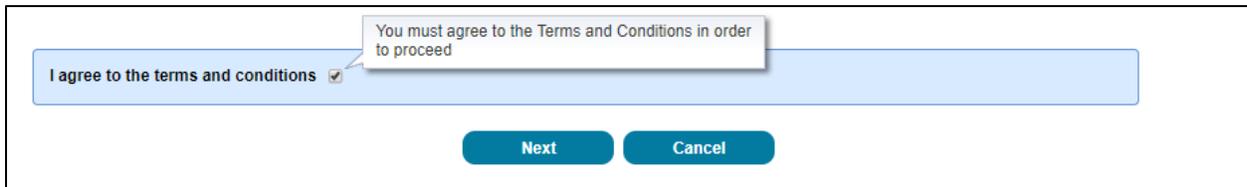
I have read the HHS Rules of Behavior for Privileged User Accounts (addendum to the HHS Rules of Behavior (HHS RoB), document number HHS-OCIO-2013-0003S and dated July 24, 2013), and understand and agree to comply with its provisions. I understand that violations of the HHS Rules of Behavior for Privileged User Accounts or information security policies and standards may lead to disciplinary action and that these actions may include termination of employment; removal or disbarment from work on federal contracts or projects; revocation of access to federal information, information systems, and/or facilities; criminal penalties; and/or imprisonment. I understand that exceptions to the HHS Rules of Behavior for Privileged User Accounts must be authorized in advance in writing by the OpDiv Chief Information Officer or his/her designee. I also understand that violation of certain laws, such as the Privacy Act of 1974, copyright law, and 18 USC 2071, which the HHS Rules of Behavior for Privileged User Accounts 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.

Figure 22: Terms & Conditions

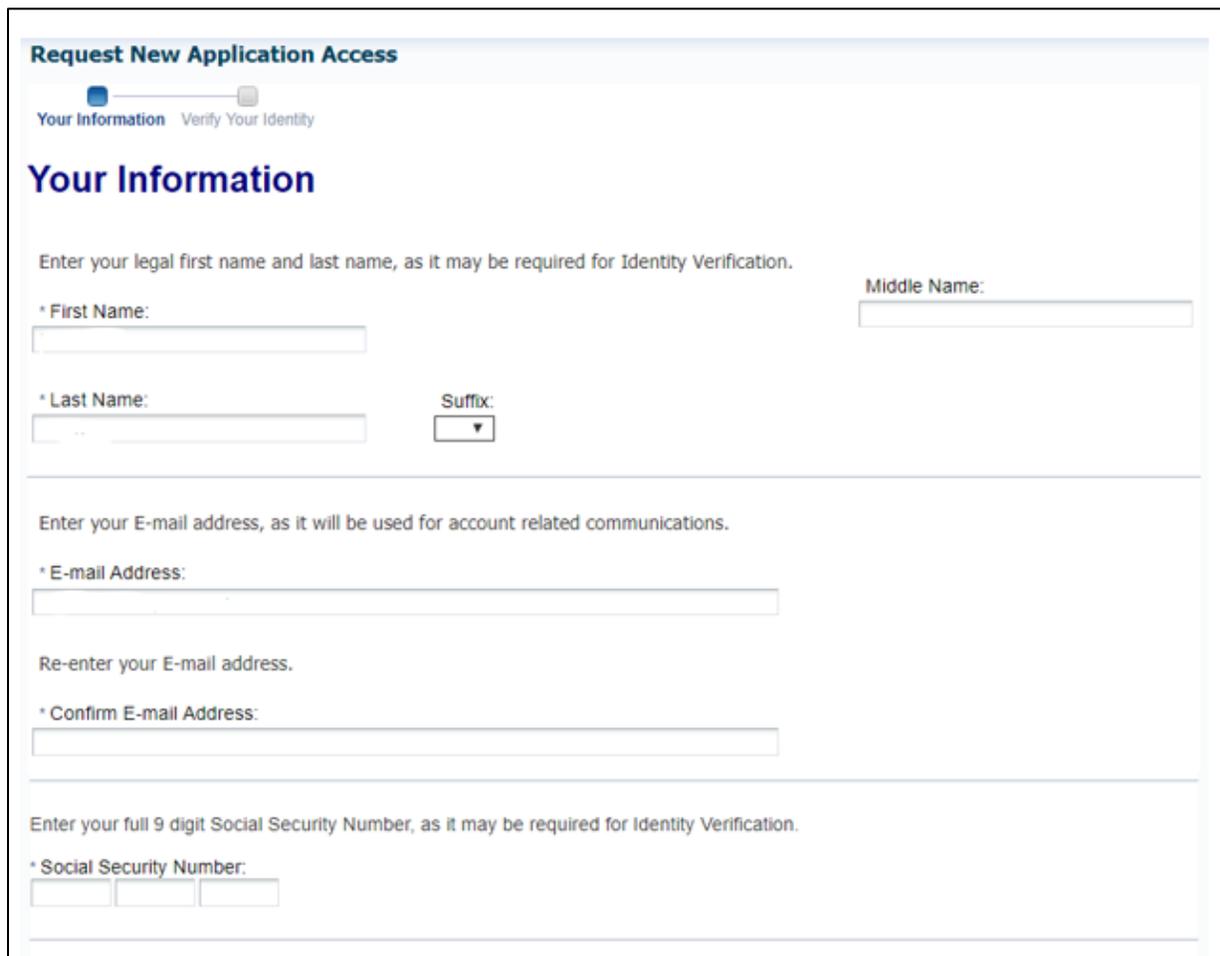
3. Indicate agreement by selecting the checkbox that states “**I agree to the terms and conditions.**” Select the **Next** button to continue with the registration process. The button is disabled until you select the checkbox.



The screenshot shows a light blue rectangular area containing a checkbox labeled "I agree to the terms and conditions" which is checked. To the right of the checkbox is a tooltip box with the text "You must agree to the Terms and Conditions in order to proceed". Below the checkbox area are two teal buttons: "Next" and "Cancel".

Figure 23: Agree to Terms & Conditions

4. The **Your Information** page is displayed. Information previously entered during the Enterprise Portal registration process will be pre-filled on this page. Complete the remaining required fields on this page and click **Next** to continue the Identity Verification process.



The screenshot shows a web page titled "Request New Application Access". At the top, there is a progress indicator with two steps: "Your Information" (active) and "Verify Your Identity". Below the title, the heading "Your Information" is displayed. The page contains several form fields:

- A prompt: "Enter your legal first name and last name, as it may be required for Identity Verification."
- Fields for: * First Name, Middle Name, * Last Name, and Suffix (a dropdown menu).
- A prompt: "Enter your E-mail address, as it will be used for account related communications."
- Fields for: * E-mail Address and * Confirm E-mail Address.
- A prompt: "Enter your full 9 digit Social Security Number, as it may be required for Identity Verification."
- Field for: * Social Security Number.

Figure 24: Your Information Page (Part 1)

Enter your date of birth in MM/DD/YYYY format, as it may be required for Identity Verification.

* Date of Birth:

U.S. Home Address Foreign address

Enter your current or most recent home address, as it may be required for Identity Verification.

* Home Address Line 1:

Home Address Line 2:

* City: * State: * Zip Code: Zip Code Extension: Country: US

Enter your primary phone number, as it may be required for Identity Verification.

* Primary Phone Number:

Figure 25: Your Information Page (Part 2)

- Each field on the **Your Information** page has a tool tip pop-up if additional instruction is needed. The tip will appear when you click in the field.

Enter your legal first name and last name, as it may be required for Identity Verification.

* First Name:

* Last Name: Suffix:

Enter your First Name. Allowed special characters are Apostrophe ('), hyphen (-), and spaces.

Figure 26: Your Information – Sample Tool Tip

6. Any missing or invalid data will be noted in an error window at the top of the **Your Information** page. Correct all errors and click **Next**.

Your Information

✖ **Error**

Messages for this page are listed below.

Social Security Number: SSN(1) ✖ Missing Value for required field Social Security Number: SSN(1). Please enter the missing information to proceed further.

SSN(2) ✖ Missing Value for required field SSN(2). Please enter the missing information to proceed further.

SSN(3) ✖ Missing Value for required field SSN(3). Please enter the missing information to proceed further.

Figure 27: Your Information – Sample Error Messages

7. Depending on the information provided, the **Verify Identity** page is displayed. You are required to answer several questions about information that may be in your personal records. Answer the questions to the best of your ability. Select the **Next** button to submit the request.

Verify Identity

You may have opened a student loan in or around September 2013. Please select the lender that you have previously or you are currently making payments to. If you have not received student loans with any of these lenders now or in the past, please select 'NONE OF THE ABOVE/DOES NOT APPLY'.

BANK ONE
 US DEPT OF EDUCATION
 GLHEC STUDENT LOAN
 FIRST SECURITY BK
 NONE OF THE ABOVE/DOES NOT APPLY

You may have opened a (HOME SAVING OF AMERICA) credit card. Please select the year in which your account was opened.

2009
 2011
 2013
 2015
 NONE OF THE ABOVE/DOES NOT APPLY

Which one of the following retail credit cards do you have? If there is not a matched retail credit card, please select 'NONE OF THE ABOVE'.

AMERICAN CREW
 KRAGEN
 SELFRIDGES
 SARAY
 NONE OF THE ABOVE/DOES NOT APPLY

Which of the following is a current or previous employer? If there is not a matched employer name, please select 'NONE OF THE ABOVE'.

SECOND CHANCE CONSIGNNE
 USC SCH OF MED
 ROYAL TIRE AND AUTO
 FAITH CONSTRUCTION
 NONE OF THE ABOVE/DOES NOT APPLY

Please select the county for the address you provided.

KOHALA
 HONOLULU
 MAUI
 KAUAI
 NONE OF THE ABOVE/DOES NOT APPLY

Figure 28: Verify Identity Page

8. After submitting the request, the Identity Verification confirmation is displayed. Select the **Next** button to continue.
9. If you receive an error message that your identity cannot not be verified, it may simply mean that the information you provided could not be matched with the information available in the electronic records used for verification. You may need to take some additional steps to verify your identity.
 - a. Check your personal information before trying again to register with the system.
 - b. If you have entered the correct information and still cannot be verified, you are instructed to call the Experian Help Desk and provide the **Review Reference Number** displayed on the screen so the help desk representative can help you verify your identity. Experian is the contractor CMS uses to complete the Identity Verification process.
 - c. After you have contacted Experian, login to CMS Enterprise Portal and proceed again through Request Access process.
 - d. On the **Your Information** screen, select the check box if you have contacted Experian and completed the identity verification process over the phone with the Experian Support personnel. Selecting this checkbox instructs the system to retrieve your identity verification results from Experian based on the phone verification process.
 - e. If your identity cannot not be verified by Experian, contact the [OH CDMS Help Desk](#) for the next steps.

5.3 Multi-Factor Authentication

1. The **Multi-Factor Authentication Information** page is displayed. Click **Next** to begin the MFA Registration process.

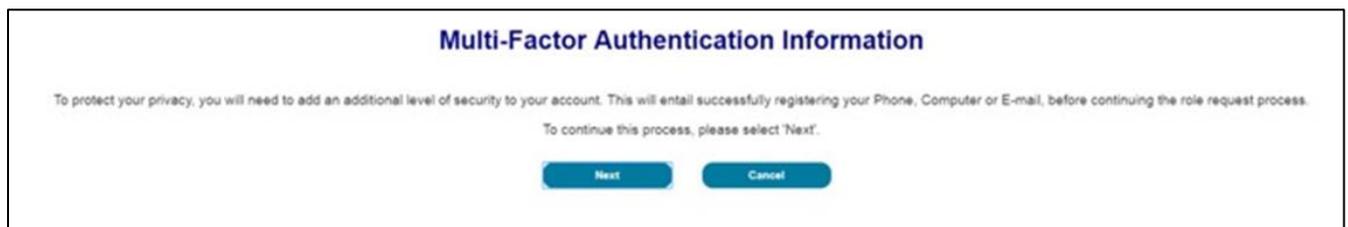


Figure 29: Multi-Factor Authentication Information Page

- The **Register Your Phone, Computer, or E-Mail** page is displayed. Review the security options.

Request New Application Access

Register Your Phone, Computer, or E-mail

Adding a Security Code to your login also known as Multi-Factor Authentication (MFA) can make your login more secure by providing an extra layer of protection to your user name and password.

You can associate the Security Code to your profile by registering your Phone, Computer or E-mail. Select the links below to find out more information about the options.

▽ **Phone/Tablet/PC/Laptop**
 To use the Validation and ID Protection (VIP) access software on your phone or computer, you must download the VIP Access software, if you do not already have it. Select the following link - <https://m.vip.symantec.com>

▽ **Text Message Short Message Service (SMS)**
 The SMS option will send your Security Code directly to your mobile device via text message. This option requires you to provide a ten (10) digits U.S. phone number for a mobile device that is capable of receiving text messages. Carrier service charges may apply for this option.

▽ **Interactive Voice Response (IVR)**
 The IVR option will communicate your Security Code through a voice message that will be sent directly to your phone. This option requires you to provide a valid ten (10) digits U.S. phone number and (Optional) extension that will be used during login to obtain the Security Code. The extension may begin with any one of the following: asterisks '*'; period '.'; comma ','; pound '#', followed by numeric 0 to 9. For example: 4885554444, 1112.

- , (comma) Creates a short delay of approximately 2 seconds;
- . (period) Creates a longer delay of approximately 5 seconds;
- * (asterisk) Used by some phone systems to access an extension; and
- # (pound/hash) Used by some phone systems to access an extension;

You may use a comma if you are not sure of the special character supported by your phone system.
To access the application, you must enter the provided Security Code on the login page. Carrier service charges may apply for this option.

✉ **E-mail**
 The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using the E-mail option. When logging into a secure application, your Security Code that is required at the login page will be E-mailed to the E-mail address on your profile.

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your device within two attempts please log out, then log back in to try again.

Select the MFA Device Type that you want to use to login to secure applications from the dropdown menu below.

MFA Device Type:

Figure 30: Register Phone, Computer, or Email for MFA Access

- Select the device type you wish to register from the **MFA Device Type** drop-down list. There are four options and each will open different fields as noted below.

The E-mail address on your profile will be used when registering for Multi-Factor Authentication (MFA) using the E-mail option. When logging into your application, your Security Code that is required at the login page will be E-mailed to the E-mail address on your profile.

Please note that you are only allowed two attempts to register your MFA device. If you are unable to register your device within two attempts please log out, then log back in to try again.

Select the MFA Device Type that you want to use for logging into your application.

MFA Device Type:

Select MFA Device Type

Phone/Tablet/PC/Laptop

E-mail

Text Message-Short Message Service(SMS)

Interactive Voice Response(IVR)

Figure 31: MFA Device Type Drop-Down Menu

4. Enter the required information to complete the MFA registration process:
 - **Phone/Tablet/PC/Laptop:** Users must download the Validation and Identity Protection (“VIP”) software from <https://m.vip.symantec.com> to their smart phone/tablet/computer. This software will generate a security code every 30 seconds that will be used at login. Enter the alphanumeric code that displays under the field labeled **Credential ID** on the VIP Access software into the **Enter Credential ID** field in the Enterprise Portal to register the device. Enter a brief description (e.g., Laptop or VIP Token) in the field labeled **MFA Device Description**.



Figure 32: VIP Access Display

* MFA Device Type: Phone/Tablet/PC/Laptop

* Credential ID : Enter the alphanumeric code that displays under the label Credential ID on your device. VSHM49586924

* MFA Device Description: VIP Access

MFA Device Description is a nick-name that can help you identify your device. You are allowed to use alphanumeric characters and special characters, such as apostrophe, dash, and period.

Figure 33: MFA Registration Fields – Phone/Tablet/PC/Laptop

- **Email:** Users can receive an email containing the security code. The email address on the user’s profile is used and will be automatically pre-filled. Enter a brief description in the field labeled **MFA Device Description**. Note that delays in e-mail transmission, spam filters, and other issues outside the user’s control can make this the least desirable option to receive a security code.
- **Text Message (SMS):** Users can have their security code texted to their phone. The user must enter a valid phone number and the phone must be capable of receiving text messages. Carrier charges may apply. Enter a brief description in the field labeled **MFA Device Description**.
- **Interactive Voice Response (IVR):** The user can receive a voice message containing their security code. The user must enter a valid phone number and (optional) phone extension. Enter a brief description in the field labeled **MFA Device Description**.

5. Select **Next** to complete the registration. A message that you have successfully registered your device is displayed. Select **Next** again to continue.

The screenshot shows a web interface with a left-hand navigation menu. Under 'My Access', there are links for 'View and Manage My Access' and 'Request New Application Access'. Under 'Requests', there are links for 'Annual Certification' and 'My Pending Requests'. The main content area is titled 'Request New Application Access' and contains a sub-header 'Register Your Phone, Computer, or E-mail'. Below this, a message states: 'You have successfully registered your Phone/Computer/E-mail to your user profile. Please select 'Next' to continue with your role request'. A blue 'Next' button is positioned at the bottom center of the main content area.

Figure 34: MFA Registration Confirmation

6. An email will also be issued indicating that you have successfully registered your Phone/Computer/E-mail.

5.4 Complete Access Request

1. The **Request New Application Access** page is displayed to review personal information that was previously entered and to update your profile information with additional business contact information.
2. Enter the requested information and select **Next**.

The screenshot shows the 'Request New Application Access' page with a form for updating profile information. The page title is 'Request New Application Access' and the sub-header is 'Please update your profile to continue the request for an application access.' The form is divided into several sections: 'Name' (with fields for Title, First Name: Susan, Middle Name, Last Name: Dobbs, and Suffix), 'Professional Credentials' (with a text field), 'Social Security Number' (with a masked field: *****3494), 'Business Contact Information' (with fields for Company Name, Address 1, Address 2, City, State/Territory, Zip Code, and Zip Code Extension), and 'Phone' (with fields for Company Phone Number and Office Phone Number, each with an Extension field). A '* Required Field' indicator is present. An 'iHelp Interactive Help' box is located on the right side, stating: 'This section will automatically update as you go through the site. It provides helpful information to ensure you easily interact with EIDM.' At the bottom right, there are 'Next' and 'Cancel' buttons.

Figure 35: Update Profile Page

- In the **Reason for Request** field, enter a brief reason why you are requesting access to OH CDMS. Select **Next**.

Request New Application Access * Required Field

Application Description: Salesforce
 CMS business applications on Salesforce Platform. Users include CMS Employees/Contractors, Applicants, Providers, Participants, State Organizations, and General Public etc.

Select a Role: Salesforce user
 Role Description: CMS Employees/Contractors, Applicants, Providers, Participants, State Organizations, and General Public etc.

* Reason for Request:

Next **Cancel**

iHelp
Reason for Request
 The 'Reason for Request' field represents the justification for submitting the request and can contain any additional comments.

Figure 36: Reason for Request

- The Request New Application Access Review page is displayed to do a final review of the entered data. Review the request, make corrections if necessary, and select **Submit**.

Request New Application Access Review * Required Field

Application Description: Salesforce
 CMS business applications on Salesforce Platform. Users include CMS Employees/Contractors, Applicants, Providers, Participants, State Organizations, and General Public etc.

Role Selected: Salesforce user
 Role Description: CMS Employees/Contractors, Applicants, Providers, Participants, State Organizations, and General Public etc.

Name
 Title: First Name: Susan Middle Name: Last Name: Dobbs Suffix:
 Professional Credentials:
 Social Security Number: *****3494

Business Contact Information
 Company Name: Actionet
 Address 1: 22 Lord Baltimore Drive
 Address 2:
 City: Baltimore
 State/Territory: Maryland
 Zip Code: 21234 Zip Code Extension:

Phone
 Company Phone Number: 734-563-7841 Extension:
 Office Phone Number: 734-563-7841 Extension:
 Reason for Request: User Training

Edit **Submit** **Cancel**

iHelp
Review
 The Review page allows you to review your request. Please select an action to continue.

Figure 37: Review Request

5. A confirmation message is displayed. Select **OK**.



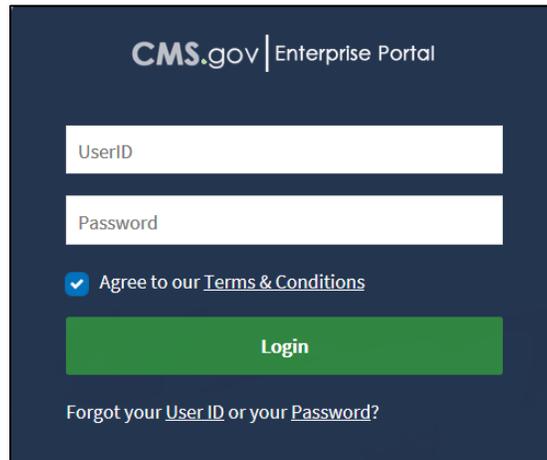
Figure 38: Request New Application Access Acknowledgement

6. An email will be issued indicating that your EIDM request has been submitted. This email will indicate the request tracking number and notes that another email will be issued when action has been taken on the request.
7. A second email will be issued indicating approval or denial of the EIDM request. Further action may not be taken until EIDM approval is granted.

6. Access the Salesforce App Store

The Salesforce App Store provides registered Salesforce Users access to applications that have integrated with the CMS Portal.

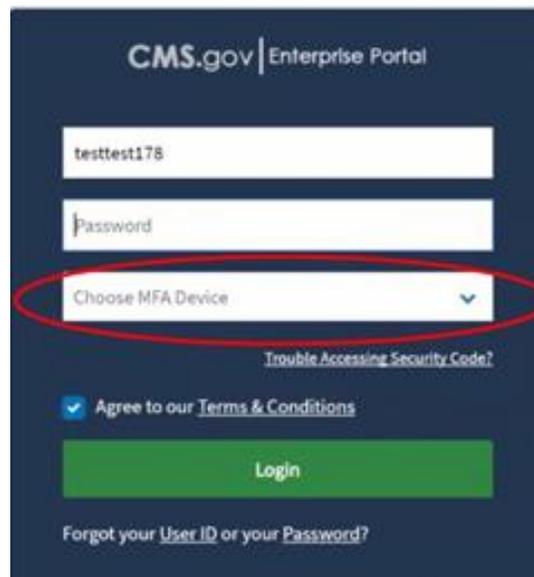
1. Navigate to <https://portal.cms.gov/>. If still logged in from the previous registration steps, you must logout and log back in using the MFA code.



The screenshot shows the login page for the CMS.gov Enterprise Portal. It features a dark blue background with white text. At the top, it says "CMS.gov | Enterprise Portal". Below this are two white input fields: "UserID" and "Password". Under the "Password" field is a checkbox labeled "Agree to our Terms & Conditions" with a blue checkmark. Below the checkbox is a green "Login" button. At the bottom, there is a link that says "Forgot your User ID or your Password?".

Figure 39: Portal Login Page

2. Enter your CMS User ID in the **UserID** field. Upon entering a username that is configured with MFA, an additional **Choose MFA Device** field with a drop-down menu is displayed.



This screenshot is similar to Figure 39, but it shows the login page after a user ID has been entered. The "UserID" field now contains the text "testtest178". A new field, "Choose MFA Device", has appeared below the "Password" field. This field is a white box with a drop-down arrow on the right side and is circled in red. Below this field is a link that says "Trouble Accessing Security Code?". The "Login" button and the "Forgot your User ID or your Password?" link are still visible at the bottom.

Figure 40: Choose MFA Device Drop-Down Menu

3. Enter the CMS password in the **Password** field.
4. Select the desired MFA Device from the drop-down menu.

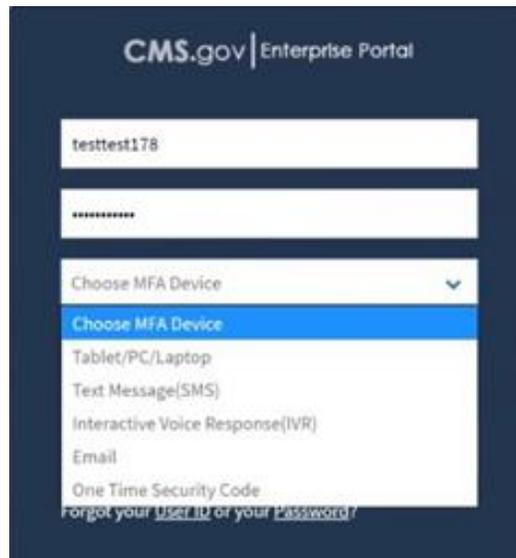


Figure 41: MFA Device Options

5. Depending on the MFA Device selected, different fields/buttons will be displayed. For text, IVR, or email options, select the **Send MFA Code** button. For the Tablet/PC/Laptop Option this step is not needed as the VIP software automatically generates the security code.
6. Retrieve the MFA code from the specified device and enter it in the **Security Code** field. Select the **Login** button.

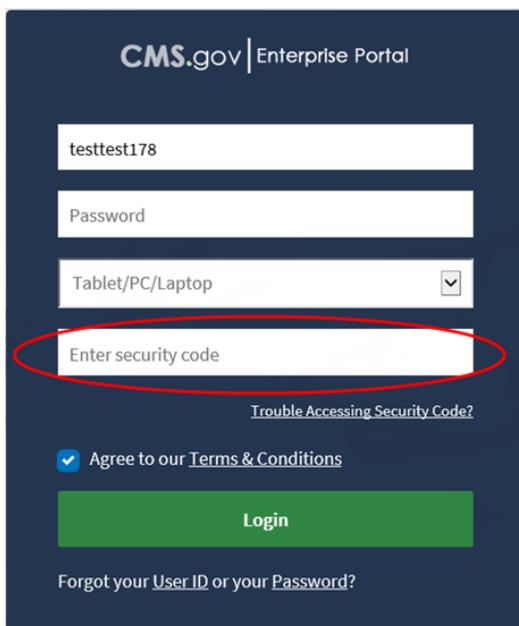


Figure 42: Selecting Tablet/PC/Laptop Option as MFA Device

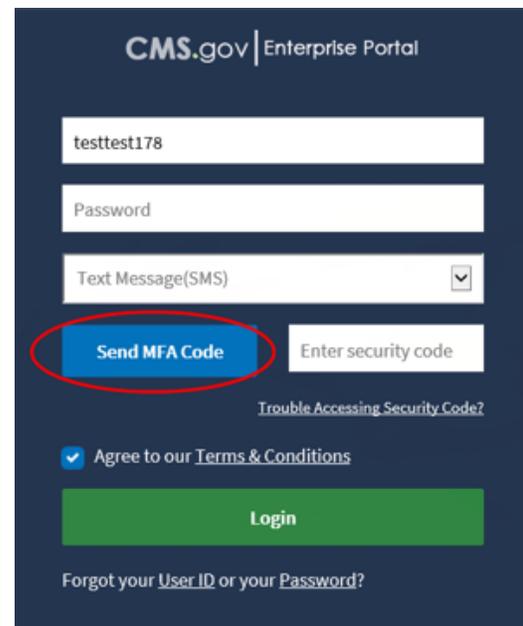
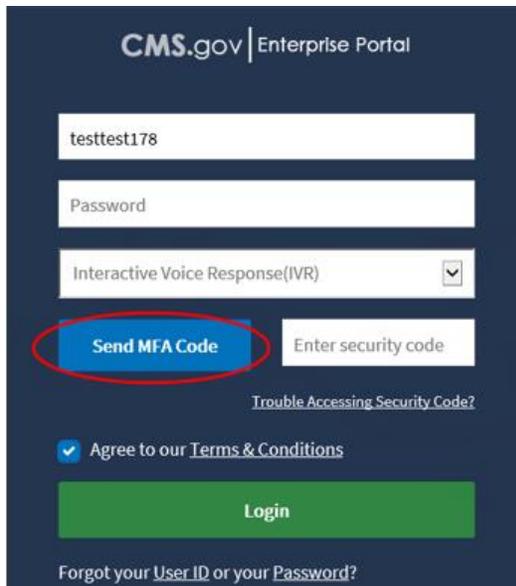
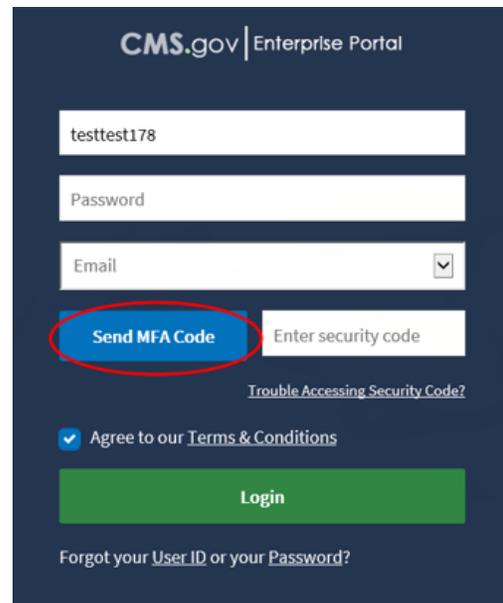


Figure 43: Selecting Text Message (SMS) as MFA Device



The screenshot shows the CMS.gov Enterprise Portal login interface. It includes a User ID field with 'testtest178', a Password field, and a dropdown menu for 'Interactive Voice Response(IVR)'. A red circle highlights the 'Send MFA Code' button. Below it is an 'Enter security code' field and a 'Login' button. There are also links for 'Trouble Accessing Security Code?' and 'Agree to our Terms & Conditions'.

Figure 44: Selecting Interactive Voice Response as MFA Device



The screenshot shows the CMS.gov Enterprise Portal login interface. It includes a User ID field with 'testtest178', a Password field, and a dropdown menu for 'Email'. A red circle highlights the 'Send MFA Code' button. Below it is an 'Enter security code' field and a 'Login' button. There are also links for 'Trouble Accessing Security Code?' and 'Agree to our Terms & Conditions'.

Figure 45: Selecting Email as MFA Device

7. The **My Portal** page is displayed. Select the **Salesforce** tile.

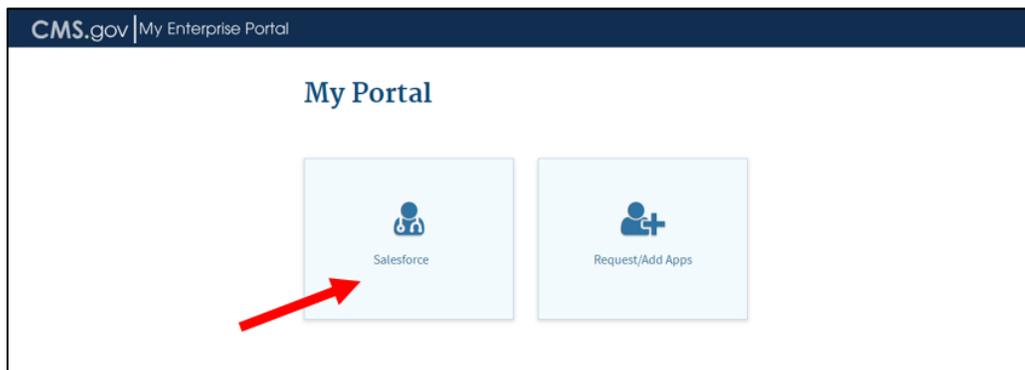


Figure 46: My Portal

8. Select the **Application** link that is listed below the **Salesforce** tile.

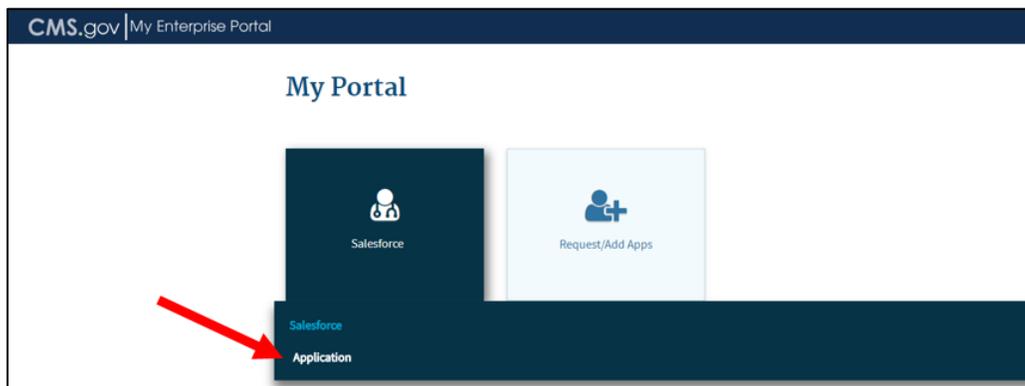


Figure 47: My Portal – Salesforce Application

9. The **CMS App Launcher** page is displayed. Select the **App Store** link.

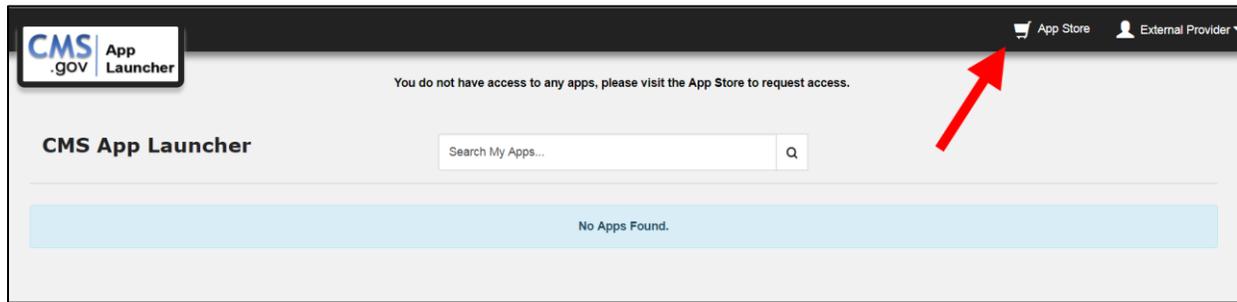


Figure 48: CMS App Launcher

10. The **App Store** is displayed with a tile for each active Salesforce Application.

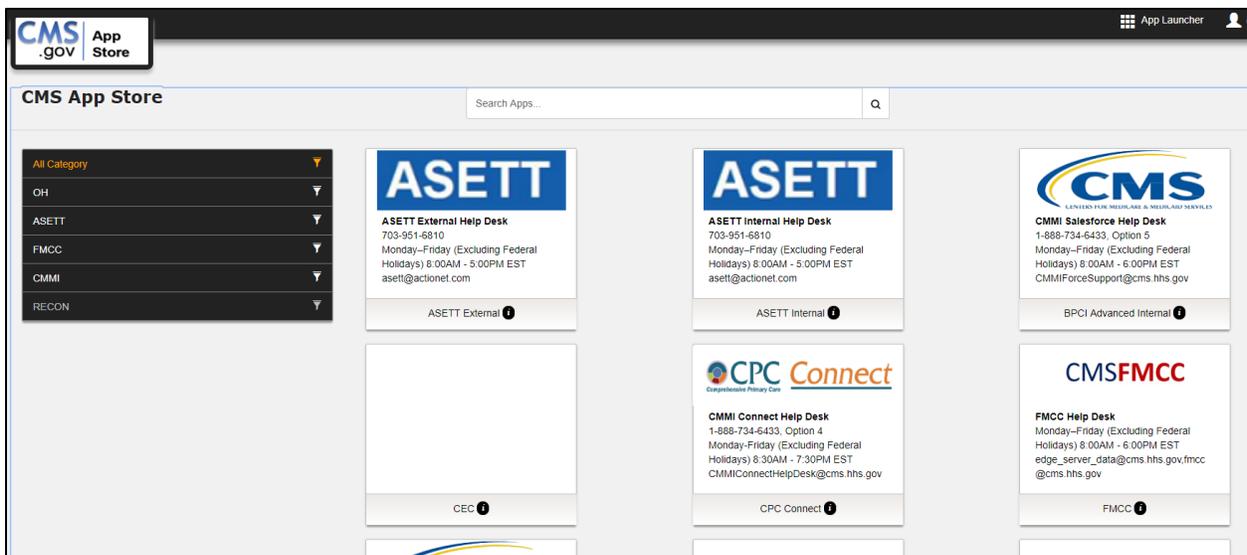


Figure 49: CMS App Store

11. Locate the **OH CDMS** App tile by: (1) selecting the OH filter in the category list; (2) typing OH into the Search Apps field; or (3) scrolling through the menu of applications.

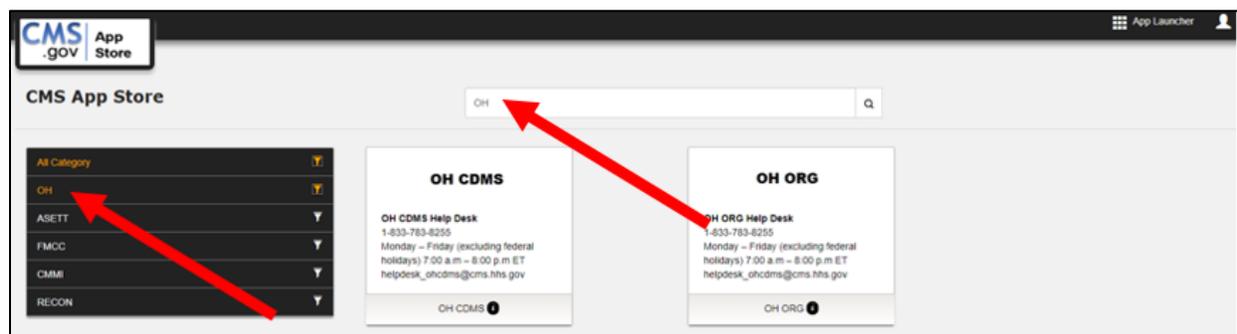


Figure 50: CMS App Store – Filtered for OH

- Click on the **OH CDMS** tile to select the application. Help Desk information is displayed on the tile for reference purposes.

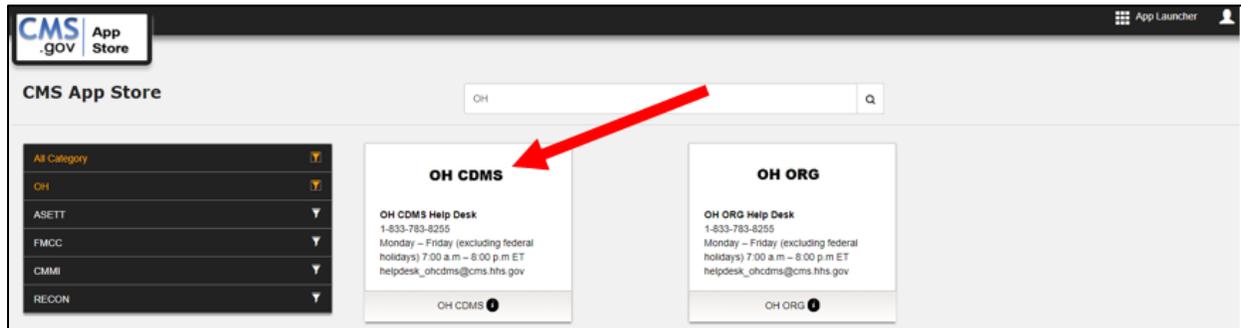


Figure 51: CMS App Store – OH CDMS Application Tile

- The **CMS App Listing** page for the selected **OH CDMS** tile is displayed. Select the **Send Request** button.

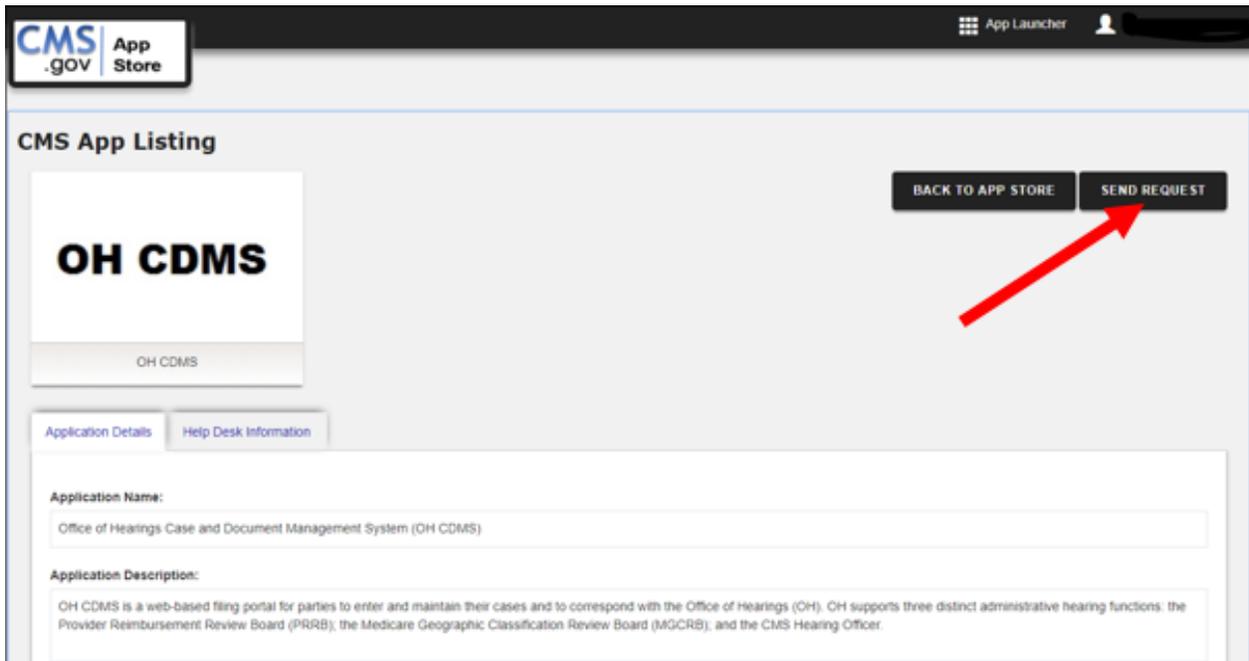


Figure 52: CMS App Listing – OH CDMS Application

14. The **Request Details** window is displayed. Within the freeform text field, describe your role and any specific module details that you are requesting access for. Select the **Send** button.

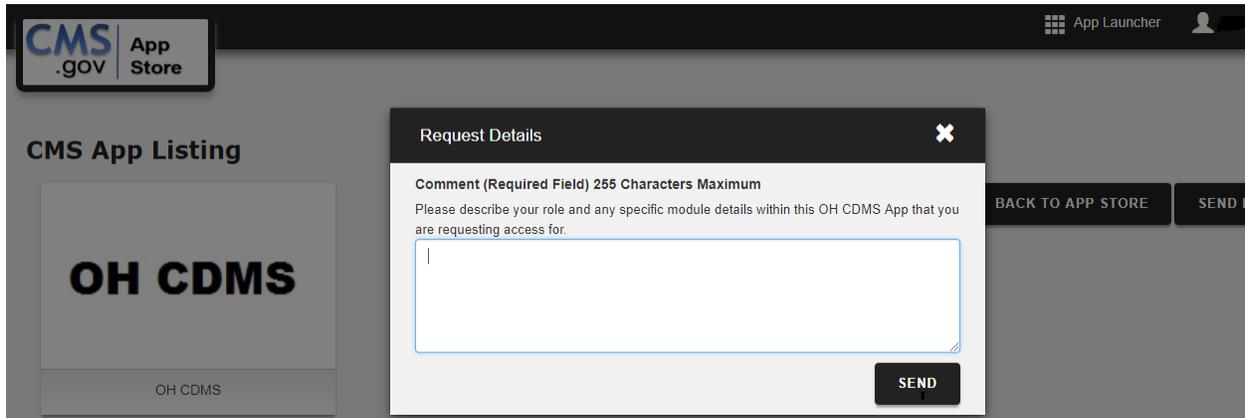


Figure 53: Request Details Window

15. An **Application Request** message is displayed. Select the **Continue** button.

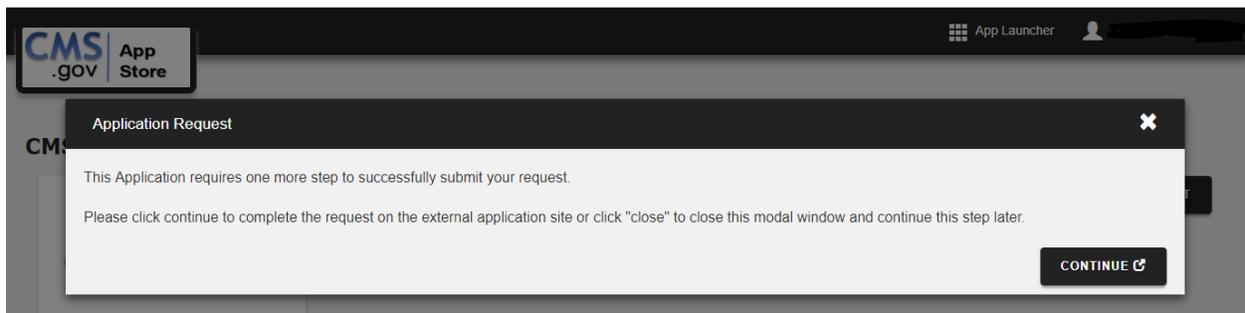


Figure 54: Application Request Confirmation

7. Request OH CDMS User Role

1. Upon successfully selecting the OH CDMS App from the Salesforce App Store, the OH CDMS Community Registration page is displayed.
2. Enter text into the fields and make selections from drop-down menus as requested. This information is specific to OH CDMS and is the manner with which the PRRB, MGCRB, and/or CMS Hearing Officer will correspond with you regarding your cases.

CMS.gov
Centers for Medicare & Medicaid Services

Office of Hearings Case and Document Management System Community Registration

All information entered below must be business information and not personal.
Your request will not be processed if you click the back button or navigate from the page.
All fields are required unless noted as optional.

Contact Information

Prefix
Select Prefix

First Name
External

Last Name
Provider

Suffix (Optional)
None

Job Title
Type Job Title

Business Mailing Address
Type Business Mailing Address

City
Type City

State
Select State

ZIP Code
Type ZIP Code

Business Phone Number
Type Business Phone Number

Business Email
Type Business Email

Requester Organization Type
Select One

Submit Request

Figure 55: Community Registration Page

3. Select the desired user role from the **Requester Organization Type** drop-down menu.

Requester Organization Type

Provider Organization ▼

Select One

Provider Organization

Parent Organization

Hearing Office Petitioner

Representative Organization

Medicare Administrative Contractor

Appeals Support Contractor

Centers for Medicare & Medicaid Services

Submit Request

Figure 56: Requester Organization Type Drop-Down Menu

- a. If you select Hearing Officer Petitioner from the **Requester Organization Type** drop-down menu, then an additional field is displayed to select the **Hearing Office Petitioner Type**. Make a selection from the second drop-down menu and then the **Organization Information** section will be displayed.

Requester Organization Type

Hearing Office Petitioner ▼

Hearing Office Petitioner Type

Select One

Medicare Advantage Organization

Representative Organization

State/Territory Agency

Other

Submit Request

Figure 57: Hearing Officer Petitioner Type Drop-Down Menu

- b. If you select any other organization type from the drop-down list, then the **Organization Information** section will automatically be displayed.
4. Start typing your organization's name in the resulting organization information field. When at least two letters have been entered, the field will present a predictive text drop-down list. The volume of entries on the list will decrease as more characters are entered. You must select the appropriate organization entry from the predictive list to complete the field.

Organization Information

Provider Name/Number

Test Organiz

I don't see my organization. I would like to create a new organization.

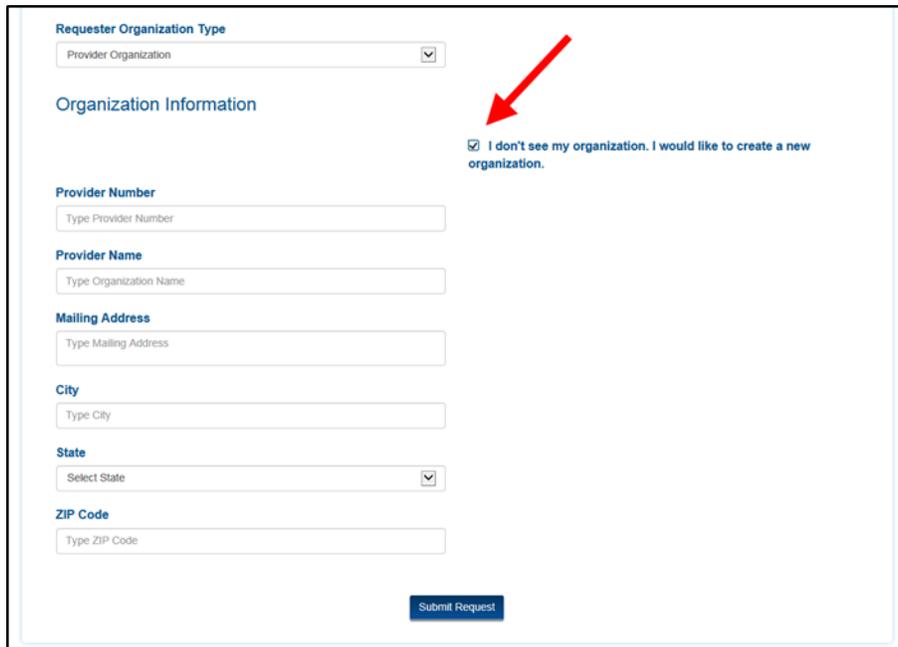
Red Glove Test Organization (76-7678)

Test Organization (87-8787)

Submit Request

Figure 58: Organization Information Page

5. If your organization does not exist in the system, select the checkbox that says “I don’t see my organization. I would like to create a new organization.” Additional fields are displayed. Enter text as requested.



The screenshot shows a registration form with the following sections and fields:

- Requester Organization Type:** A dropdown menu with "Provider Organization" selected.
- Organization Information:** A section containing a checkbox labeled "I don't see my organization. I would like to create a new organization." which is checked. A red arrow points to this checkbox.
- Provider Number:** A text input field with the placeholder "Type Provider Number".
- Provider Name:** A text input field with the placeholder "Type Organization Name".
- Mailing Address:** A text input field with the placeholder "Type Mailing Address".
- City:** A text input field with the placeholder "Type City".
- State:** A dropdown menu with "Select State" selected.
- ZIP Code:** A text input field with the placeholder "Type ZIP Code".
- Submit Request:** A blue button at the bottom right.

Figure 59: Community Registration Page – New Organization Fields

Note: Government entities and contractors cannot create new organizations from the registration page. You must select from the established organizations or contact the OH CDMS help desk.

6. Once you have completed all of the fields and made selections from the drop-down menus, select the **Submit Request** button. The **Application Request Confirmation** is displayed.

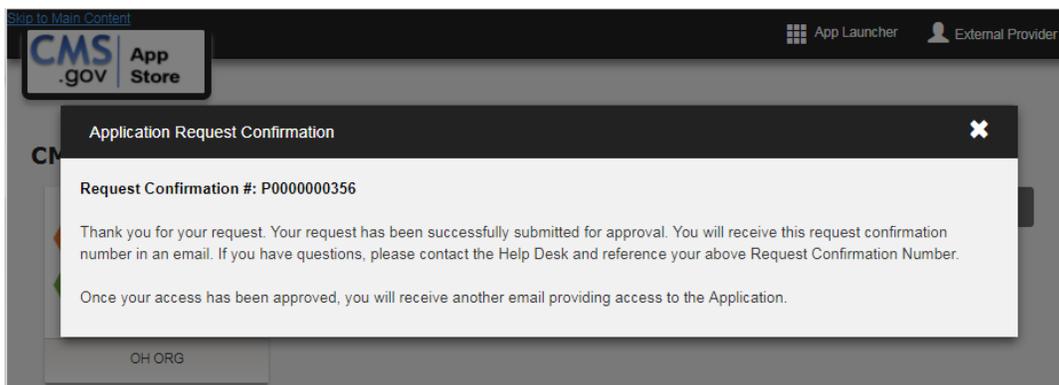
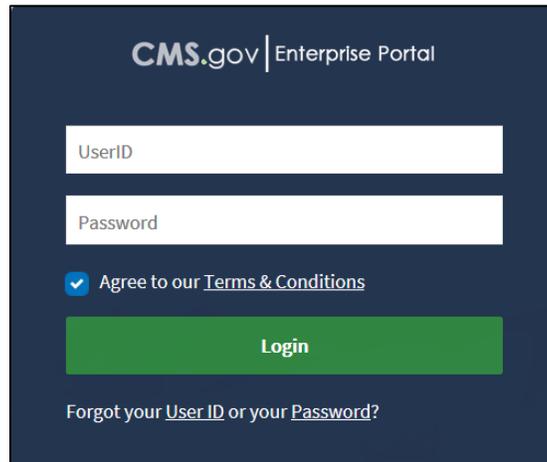


Figure 60: Application Request Confirmation

7. An email will be issued indicating approval or denial of the OH CDMS request. Further action may not be taken until OH CDMS approval is granted.

8. Launch OH CDMS

1. Navigate to the EIDM portal: <https://portal.cms.gov/>.
2. Enter User ID, Password, and MFA Security Code.



The screenshot shows the login page for the CMS.gov Enterprise Portal. It features a dark blue header with the CMS.gov logo and the text 'Enterprise Portal'. Below the header are two white input fields for 'UserID' and 'Password'. A blue checkmark icon is next to the text 'Agree to our Terms & Conditions'. A green 'Login' button is positioned below the input fields. At the bottom, there is a link that says 'Forgot your User ID or your Password?'.

Figure 61: Login Page

3. Select the **Login** button.
4. The **My Portal** page is displayed. Select the **Salesforce** tile.

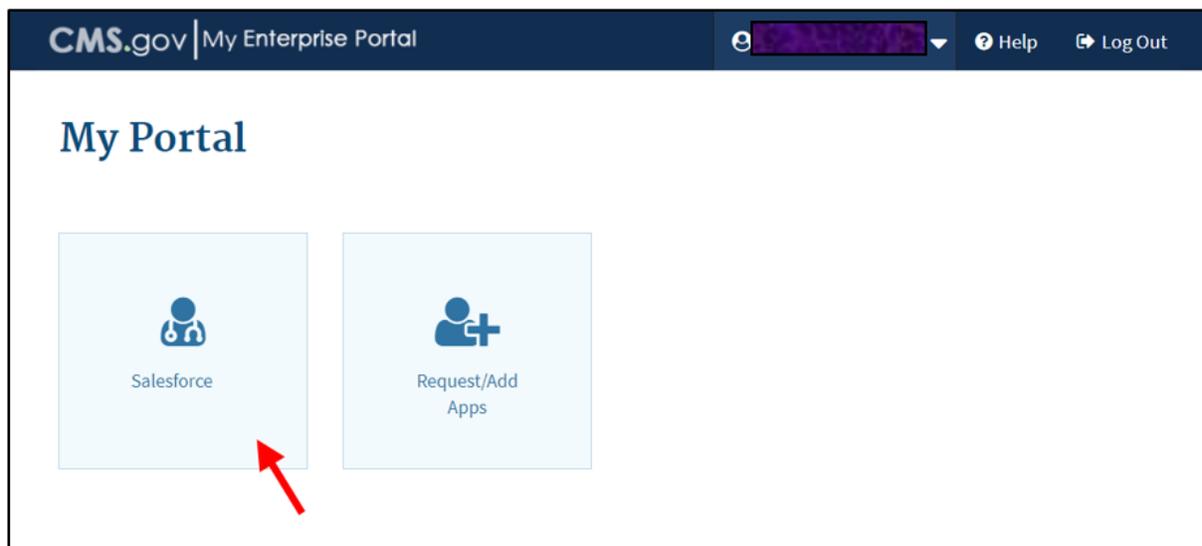


Figure 62: My Portal

5. The **CMS App Launcher** page is displayed. Select the desired OH CDMS tile to open the application.

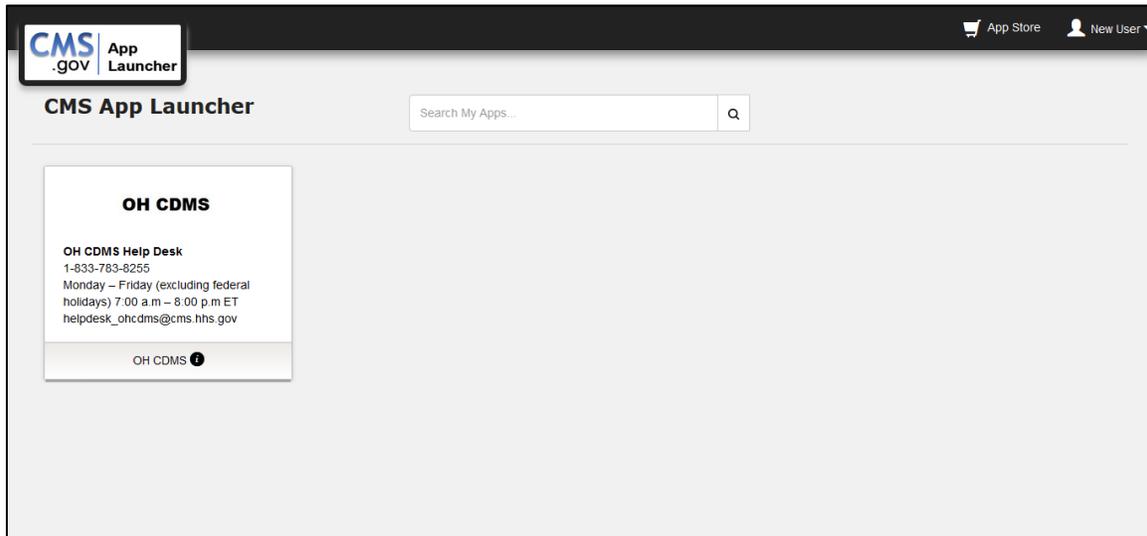


Figure 63: CMS App Launcher

- The **OH CDMS Community Rules of Behavior** page is displayed. Review the disclosures and select the **Accept** button to proceed to the OH CDMS Landing Page.



CMS.gov
Centers for Medicare & Medicaid Services

Office of Hearings Case and Document Management System Community Rules of Behavior

The Information System:

You are accessing a U.S. Government Information system, which includes 1. this computer, 2. this computer network, 3. all computers connected to this network, and 4. all devices and storage media attached to this network or to a computer on this network.

This Information system is provided for U.S. Government-authorized use only.

Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties.

By using this Information system, you understand and consent to the following:
You have no reasonable expectation of privacy regarding any communication or data transiting or stored on this Information system. At any time, and for any lawful Government purpose, the government may monitor, intercept, and search and seize any communication or data transiting or stored on this Information system.

Any communication or data transiting or stored on this Information system may be disclosed or used for any lawful Government purpose.

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. Sections 1001 and 1030. We encourage you to read the [HHS Rules of Behavior](#) for more details.

CMS will safeguard the information provided to us in accordance with the Privacy Act of 1974, as amended (5 U.S.C. Section 552a). For more information, please see the [CMS Privacy Policy](#).

Technical and Accessibility Issues: Please contact the Office of Hearings Case and Document Management System Help Desk at 1-833-783-8255 or Helpdesk_OHCDMS@cms.hhs.gov. If you are using Internet Explorer, please make sure the browser you are using is IE 9 or higher, before attempting to navigate through this site. Prior versions of IE are not supported by this system.



A federal government website managed by the Centers for Medicare & Medicaid Services
7500 Security Boulevard, Baltimore, MD 21244



Figure 64: OH CDMS Community Rules of Behavior

7. The **OH CDMS Landing Page** is displayed. The view may have one or more of the tiles noted below based on your role.

CMS.gov
Centers for Medicare & Medicaid Services

7/6/2018 - 6:49:39 PM EDT
Welcome Subhasavithri Janarathanan

Office of Hearings Case and Document Management System

Introduction:

The Office of Hearings Case and Document Management System ("OH CDMS") is a web-based filing portal for parties to enter and maintain their cases and to correspond with the Office of Hearings ("OH"). OH supports three distinct administrative hearing functions:

- The **Provider Reimbursement Review Board ("PRRB")**: provider appeals of cost report audits and other contractor determinations per 42 C.F.R. § 405, Subpart R;
- The **Medicare Geographic Classification Review Board ("MGCRB")**: hospital applications to request geographic redesignation to an alternative payment area per 42 C.F.R. § 412, Subpart L; and
- The **CMS Hearing Officer**: diverse range of matters brought by healthcare institutions, insurance issuers, state Medicaid plans, organ procurement organizations, and other entities per various regulatory authorities.

Access to the various modules is granted as needed based on role. Access to specific cases is limited to the parties of each case.

Administration **PRRB** **MGCRB** **CMS Hearing Officer**

Figure 65: OH CDMS Landing Page

8. For further information about a specific module, please reference the associated External User Manuals from the PRRB, MGCRB, and CMS Hearing Officer websites.

9. Support

9.1 OH CDMS Helpdesk

For any technical system issues, please contact the OH CDMS Help Desk at 1-833-783-8255 or email helpdesk_ohcdms@cms.hhs.gov. The hours of operation are Monday – Friday (excluding federal holidays) from 7:00 a.m. to 8:00 p.m. Eastern Time.

9.2 CMS Enterprise Portal Reference Materials

Reference the **CMS Enterprise Portal Frequently Asked Questions** (“FAQs”) at: <https://portal.cms.gov/wps/portal/unauthportal/help/>. These FAQs include a link to the **CMS Enterprise Portal User Manual**.

See also the CMS.gov EIDM Guides and Documentation webpage at: <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/EnterpriseIdentityManagement/Guides-and-Documents.html>.

Appendix A: Acronyms

Acronym	Term
CMS	Centers for Medicare & Medicaid Services
EIDM	Enterprise Identity Management
FAQs	Frequently Asked Questions
IVR	Interactive Voice Response
MFA	Multifactor Authentication
MGCRB	Medicare Geographic Classification Review Board
OH	Office of Hearings
OH CDMS	Office of Hearings Case and Document Management System
PRRB	Provider Reimbursement Review Board
SMS	Short Message Service
VIP	Validation & ID Protection

Table 1: Acronyms

Appendix B: Record of Changes

Version Number	Date	Description of Change
1.0	07/09/2018	Initial issuance for release of OH CDMS

Table 2: Record of Changes