

Health Plan Management System (HPMS) Logon Instructions

Setting Up Multi-Factor Authentication (MFA) for the First Time

1. In your web browser, enter <https://hpms.cms.gov> in the address bar. You will be taken to the HPMS landing page (see Figure 1).
2. On the HPMS landing page, enter your CMS-issued user ID (4 digits) and password (8 digits) in the appropriate fields. Select the **Log In** button to proceed.

Figure 1: HPMS Landing Page

HPMS | Health Plan Management System

JDOE ***** Log In

Helping plans navigate the Medicare Advantage and Part D programs

Want to learn more and stay on top of MA and Part D program news? Join the HPMS email list.

Subscribe to the Listserv

Announcements

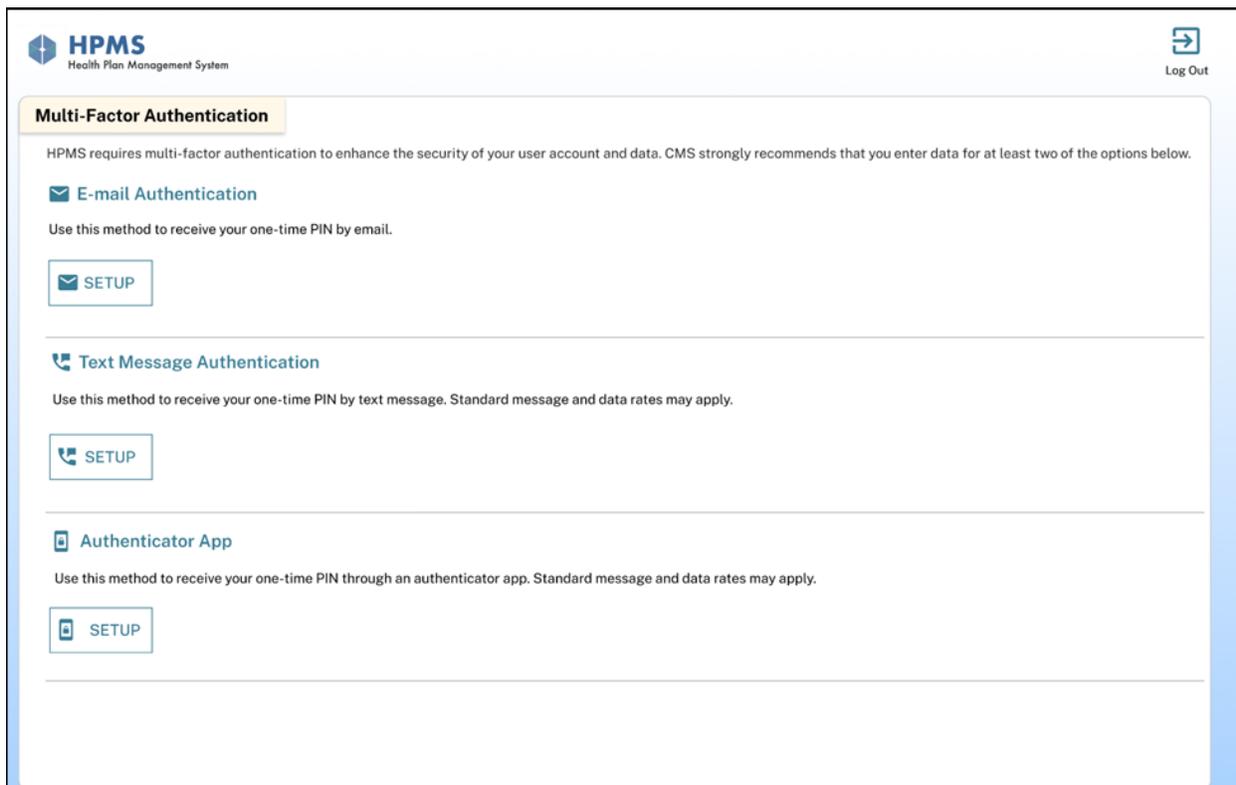
Last Updated 2 days ago

- PDPFS level three outlier processing has completed. 01/01/2020
- Drug pricing attestations due by 2:00 p.m. 01/03/2020
- Take our HPMS customer satisfaction survey. Window closes at 5:00 pm ET on January 17. 01/06/2020 - 01/17/2020
- Take our HPMS customer satisfaction survey. Window closes at 5:00 pm ET on January 17. 01/06/2020 - 01/17/2020
- Take our HPMS customer satisfaction survey. Window closes at 5:00 pm ET on January 17. 01/06/2020 - 01/17/2020

[See more...](#)

3. The HPMS Multi-Factor Authentication set up page will display (see Figure 2).

Figure 2: HPMS MFA Initial Set Up Page



4. You must click on the **Setup** button for one or more of the three options above to establish your MFA factors.
- a. **A random PIN sent via e-mail.** This method requires users to provide a valid e-mail address that will be maintained in a new MFA settings tab in the HPMS “My Account” function. This method is the least recommended option, as e-mail can often be slower than the following two delivery mechanisms.
 - b. **A random PIN sent via text message.** This method requires users to provide a valid cell phone number that will be maintained in a new MFA settings tab in the HPMS “My Account” function.
 - c. **A time-based One Time Password (OTP).** This option uses a key generated by a mobile application installed on a cell phone, such as Google Authenticator or Microsoft Authenticator. The OTP option is often the most efficient and reliable way to access a website using MFA.
5. You must also complete three mandatory security questions (see Figure 3). These questions will be used if you are unable to log into HPMS using MFA and need to reset your account.

Figure 3: HPMS Security Questions Page

Security Questions

Please setup the mandatory security questions to help unlock your account in case of getting it locked.

Select your Security Question 1 *
--Select a Question--

Answer

Select your Security Question 2 *
--Select a Question--

Answer

Select your Security Question 3 *
--Select a Question--

Answer

[Close](#) [Submit](#)

6. After selecting the **Submit** button, you will be sent to the HPMS home page (see Figure 4).

Figure 4: HPMS Home Page

HPMS
Health Plan Management System

MALIK FARHAN | Log Out | A A A
Last logged in at 10:29 AM on April 5, 2021

[Plan Dashboard](#) | [Contract Management](#) | [Plan Bids](#) | [Plan Formularies](#) | [Monitoring](#) | [Quality and Performance](#) | [Risk Adjustment](#) | [Data Extract Facility](#) | [User Resources](#)

HPMS Memos

- 04/09/2021 [Memo](#) re: Draft Contract Year 2022 Part C Benefits Review and Evaluation.
- 04/09/2021 [Memo](#) re: Release of the 2022 Plan Benefit Package and Bid Pricing Tool Software and Related Technical Bidding Guidance for Employer/Union-Only Group Waiver Plans.
- 04/09/2021 [Memo](#) re: Actuarial User Group Calls.
- 04/09/2021 [PDF](#) re: Announcement of 2022 Hospice Capitation Rates and Final Actuarial Methodology for the VBID Model's Hospice Benefit Component.
- 04/09/2021 [Memo](#) re: CY 2022 Bid Review Out-of-Pocket Cost (OOPC) Model.
- 04/07/2021 [Memo](#) re: 2021 Frailty Scores and 2020 Health Outcomes Survey (HOS) or Health Outcomes Survey Modified (HOS-M) Activities of Daily Living (ADLs) Results.
- 04/05/2021 [HPMS Email](#) re: Office Hour: 2022 Payment Design of the Hospice Benefit Component of the VBID Model.

[More »](#)



Announcements | **My Favorites**

- 01/19/2021 - 04/13/2021 HPMS FWA Reporting module pilot window.
- 04/01/2021 The CY2021 PBP benefits data has been refreshed on cms.gov as of 04/01/2021.

[More »](#)

About HPMS | Website Accessibility | Web Policies | File Formats and Plug-Ins | Rules Of Behavior | System Requirements
CV: 1.34.0.0.2



Logging into HPMS After MFA Set Up

1. On the HPMS landing page at <https://hpms.cms.gov>, enter your CMS-issued user ID (4 digits) and password (8 digits) in the appropriate fields. Select the **Log In** button to proceed.
2. Choose your one-time PIN (OTP) option, and select the **Request One-Time PIN** button.

Figure 5: Select Method to Receive OTP Page

Select Method to Receive your One-Time PIN to Login ×

To enhance security, we require a one-time PIN to complete your login to HPMS. Please select one or more methods to receive your one-time PIN:

E-Mail (pr*****.****@*****.com) - Default

Text Message (*****2614) - Secondary

Authenticator App - Secondary

You will need to enter the one-time PIN on the next page to complete your login. You must complete the login within 10 minutes of receiving your one-time PIN. If you fail to do so, your PIN will expire and you will need to reinitiate the login process by entering your ID and password.

If you do not have access to any of the verification option(s) listed on this page, contact us at 1-800-562-1963 and we will reset your account.

3. Enter your OTP on the following page (see Figure 6). You also have the option to remember the OTP on the specific browser on your device for the remainder of the day.

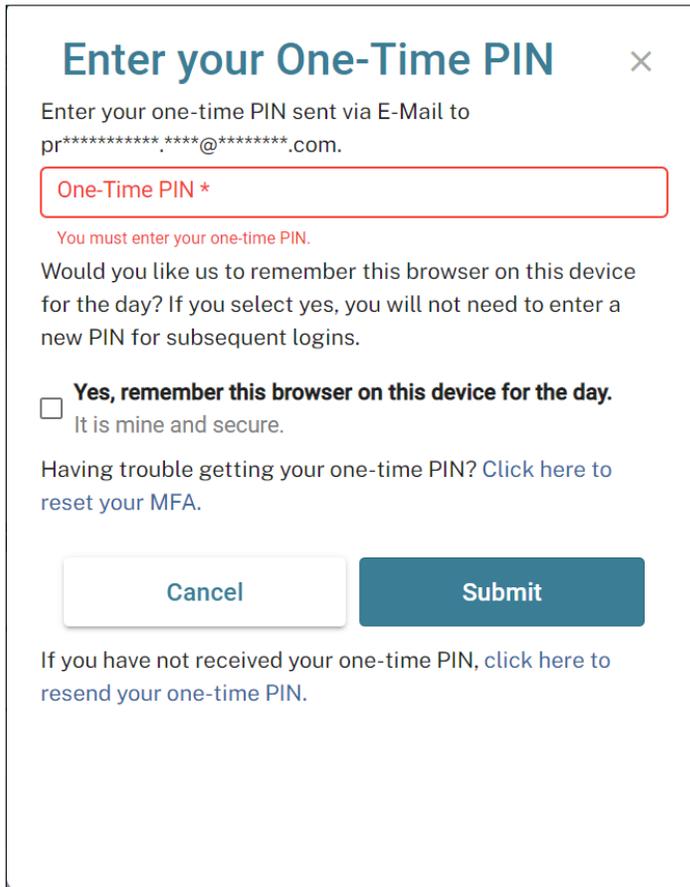
Figure 6: Enter the OTP Page

4. After selecting the **Submit** button, the HPMS home page displays.

Updating MFA Settings

1. If you are unable to complete MFA successfully, select the **Click here to reset your MFA** link (see Figure 7).

Figure 7: Reset MFA Page



The image shows a dialog box titled "Enter your One-Time PIN" with a close button (X) in the top right corner. The text inside the dialog box reads: "Enter your one-time PIN sent via E-Mail to pr*****.****@*****.com." Below this is a text input field with a red border and the placeholder text "One-Time PIN *". Underneath the input field is a red error message: "You must enter your one-time PIN." The next line of text asks: "Would you like us to remember this browser on this device for the day? If you select yes, you will not need to enter a new PIN for subsequent logins." Below this is a checkbox followed by the text: "Yes, remember this browser on this device for the day. It is mine and secure." Further down, there is a link: "Having trouble getting your one-time PIN? Click here to reset your MFA." At the bottom of the dialog box are two buttons: "Cancel" and "Submit". Below the dialog box, there is a link: "If you have not received your one-time PIN, click here to resend your one-time PIN."

2. You will be directed to complete your HPMS security questions (see Figure 8).

Figure 8: Modify HPMS Security Questions Page

Health Plan Management System Log Out

Multi-Factor Authentication

Security Questions

Please answer the security questions to reset your MFA.

1. What is the maiden name of your Mother?

Answer

2. What is the last 5-digits of your drivers license?

Answer

3. What is the name of your high school?

Answer

3. After successfully submitting your responses, you will be directed to setup your MFA options and proceed with the log on process once again.

Updating the MFA Method

You can update your MFA methods at any time using the **My Account** module under the User Resources menu.

1. To start, use the **MFA Setup** link on the Multi-Factor Authentication tab (see Figure 9).

Figure 9: HPMS User Account Management Page

HPMS Health Plan Management System TEST PRIYADARSHINI NAIR | Log Out | A A A
Last logged in at 11:51 AM on July 1, 2021

Plan Dashboard Contract Management Plan Bids Plan Formularies Monitoring Quality and Performance Risk Adjustment Data Extract Facility User Resources

Home

User Account Management

My Favorites User Account User Access Report Multi-Factor Authentication

You may review and update your HPMS multi-factor information by visiting this page: [MFA Setup](#).

You can update your e-mail address, cell phone number, or software authentication tool at any time.

- You will then be directed to the Multi-Factor Authentication set up page where you can update your MFA methods and security questions (see Figure 10).

Figure 10: HPMS MFA Method Update Page

HPMS
Health Plan Management System

Home My Account FAQs Contact Us Log Out

Multi-Factor Authentication

HPMS requires multi-factor authentication to enhance the security of your user account and data. CMS strongly recommends that you enter data for at least two of the options below.

E-mail Authentication
Use this method to receive your one-time PIN by email. (pr*****@*****.com)

Set as the primary (default) verification method

Text Message Authentication
Use this method to receive your one-time PIN by text message. Standard message and data rates may apply. (*****2614)

Set as the primary (default) verification method

Authenticator App
Use this method to receive your one-time PIN through an authenticator app. Standard message and data rates may apply.

Set as the primary (default) verification method

Security Questions

Please establish your security questions in order to reset your multi-factor authentication settings in the future.

Select your Security Question 1
If you were a car, what kind of car would you be?

Answer *

Select your Security Question 2
If you were a tree, what kind of tree would you be?

Answer *

Select your Security Question 3
What is your maternal grandmother's maiden name?

Answer *

CMS Default Password

Your default password is the first two letters of your last name (first letter capitalized) followed by the last six digits of your social security number (SSN). Please refer to the example below (where N below represents a number):

Sample User Name: John Smith Sample SSN: NNN-NN-NNNN

CMS Default Password: Sm456789

Users should change their default password upon receipt of their CMS user ID via the “Change My Password” menu item in the EUA system at <https://eua.cms.gov>.

Annual CMS User ID Recertification Process

CMS user IDs must be recertified electronically on an annual basis using CMS' System Access Certification (SAC) application at <https://eua.cms.gov/eurekify/portal/login>. For assistance with the SAC, the security computer-based training (CBT), and passwords, please contact the **CMS IT Service Desk at 1-800-562-1963 or 410-786-2580**.

If you do not complete the recertification in a timely manner, your CMS user ID will be revoked, and you will have to re-apply as a new user.

Upon receipt of a recertification email notice from eua@cms.hhs.gov, you must complete both Steps 1 and 2:

Step 1: System Access Review

1. Log into the SAC at <https://eua.cms.gov/eurekify/portal/login> using your HPMS credentials.
2. If you find a certification item on your home screen, select the "Certify" button to proceed.
3. Select the check box that appears next to your name. This action will automatically select the check boxes for all of your associated job codes.
4. Select the "Keep" button in order to retain access to the selected job codes.
5. On the summary page, select the "Submit" button to continue.
6. On the confirmation pop-up window, select the "X" that appears in the upper right hand corner in order to complete the system access review step.

Step 2: Security Training

1. Access the CMS security CBT (Information Systems Security and Privacy Awareness Training) at the following URL: <https://www.cms.gov/cbt/login/>
2. Log in using your CMS credentials and complete the training.
3. Click the "Information Systems Security and Privacy Awareness Training" link.
4. Click the "Click here for CMS Information Systems Security and Privacy Awareness (ISSPA) Training" link. Then select the "Click to launch the course" link.
5. Once complete, click the "Click to complete Course" button and print a copy of your certificate for your records, as it may be needed later in the process. Please note that you may need to log in a second time in order to generate your certificate. Your CBT is not considered to be complete until you obtain the certificate.

Step 3: Checking Your Status

You can check your System Access Review (SAC) and security CBT status in EUA at any time.

1. Log into EUA at <https://eua.cms.gov> using your HPMS credentials.
2. Click on the "View My Identity" button or use the link from the left hand navigation bar under the "Home" header.
3. Your identity information will appear on the subsequent page.

If the SAC Recert Status is "OK," the SAC Recert Completion Date has changed to the day you completed your system access review, and the SAC Recert Due Date changed to the following year, you have completed the system access review step successfully.

If the SAC Recert Status is "Pending," you have completed the system access review, but it is pending CMS

approval.

If the SAC Recert Status is "Due," you must complete the system access review as described in Step 1 above. Upon completion, your system access review will be sent to CMS for approval.

If your CBT Recert Status is "OK," you have completed the CBT and no further action is required on this step. The CBT Completion date should reflect the day you completed your CBT, while the CBT Recert Due Date should reflect the following year.

If your CBT Recert status is "Due," you must complete the security CBT as described in Step 2 above. Please note that your CBT status will be updated overnight, not immediately. However, if the CBT status remains unchanged, send a copy of your CBT certificate to CBT@cms.hhs.gov and request that CMS update your CBT status manually in EUA.

For additional information, please visit: <https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/HPMS/RecertAndPwdProcess.html>.

Password Maintenance

CMS passwords must be reset every 60 days. You can reset your CMS password using CMS' EUA system. You can access EUA over the Internet at <https://eua.cms.gov>. To change your password, select the "Change My Password" link in the left menu and follow the instructions listed on the page.

For technical assistance with this process, please contact the CMS IT Service Desk at either 1- 800-562-1963 or 410-786-2580. If your account locks and your password must be reset by the CMS IT Service Desk, your password will be reset to the default (i.e., first letter of your last name in upper case, second letter of your last name in lower case, followed by the last six digits of your social security number). You are required to change the default password immediately via EUA.

Please note that the HPMS Help Desk cannot reset passwords.

Help Resources

For HPMS user access changes, please contact the HPMS user access team at hpms_access@cms.hhs.gov.

For technical assistance with HPMS, please contact the HPMS Help Desk at either hpms@cms.hhs.gov or 1-800-220-2028.

For password issues, please contact the CMS IT Service Desk at either 410-786-2580 or 1-800-562-1963.