



HPMS – MULTI-FACTOR AUTHENTICATION (MFA) SET UP USER GUIDE

TABLE OF CONTENTS

Initial Setup.....	1
Setting Up Multi-Factor Authentication (MFA) for the First Time.....	1
Logging In After Setting Up MFA.....	4
Resetting the MFA.....	6
Updating the MFA Method.....	8

TABLE OF FIGURES

Figure 1: HPMS Landing Page	1
Figure 2: HPMS MFA Initial Set Up Page	2
Figure 3: HPMS Security Questions Page	3
Figure 4 : Select Method to Receive OTP Page	4
Figure 5: Enter your OTP Page.....	5
Figure 6: Reset your MFA link.....	6
Figure 7: Modify HPMS Security Questions Page.....	7
Figure 8: HPMS User Account Management Page	8
Figure 9: HPMS MFA Method Update Page	9

INITIAL SETUP

SETTING UP MULTI-FACTOR AUTHENTICATION (MFA) FOR THE FIRST TIME

1. Access the HPMS landing page at the following URL: <https://hpms.cms.gov>
2. On the HPMS landing page, log in using your CMS EUA ID and password.

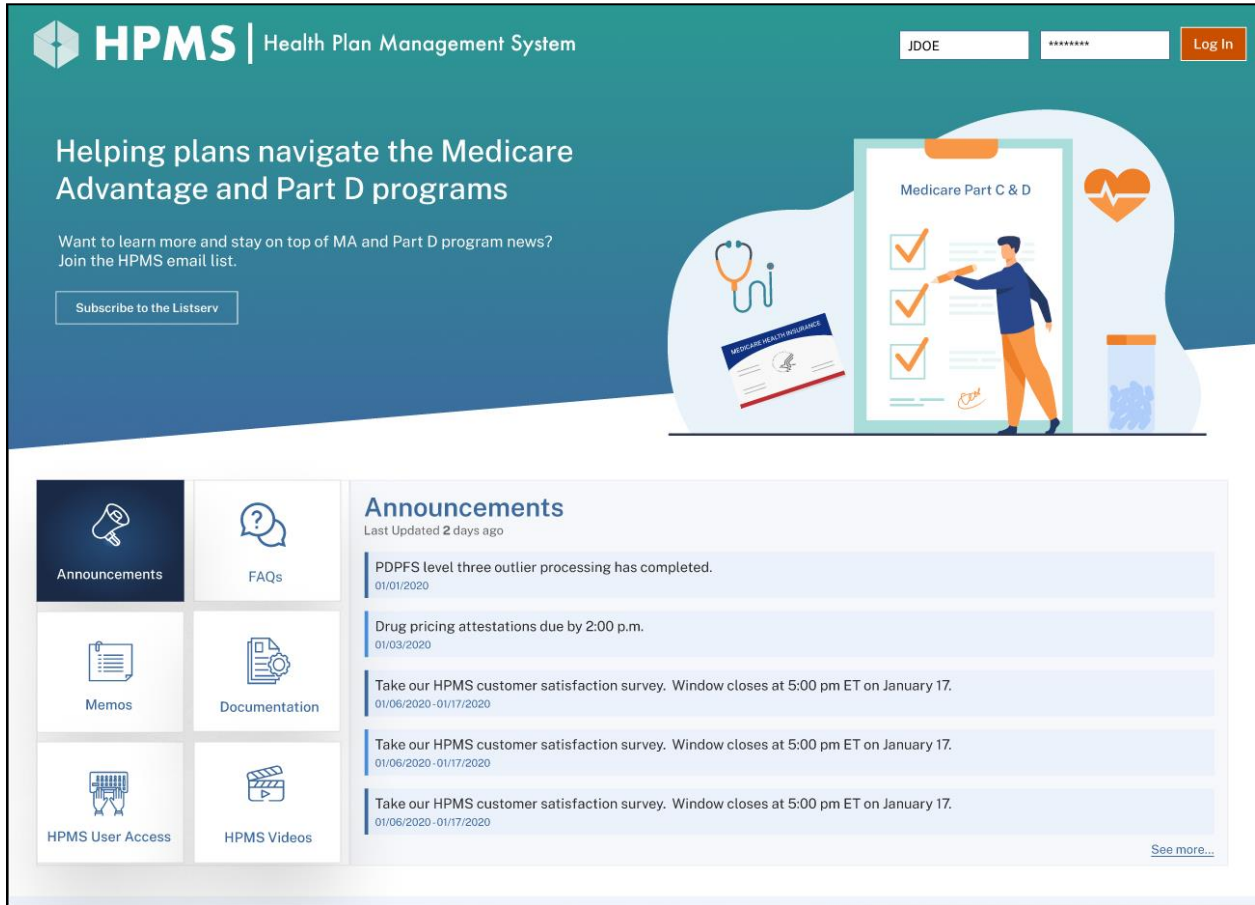


Figure 1: HPMS Landing Page

3. The HPMS Multi-Factor Authentication set up page will display.

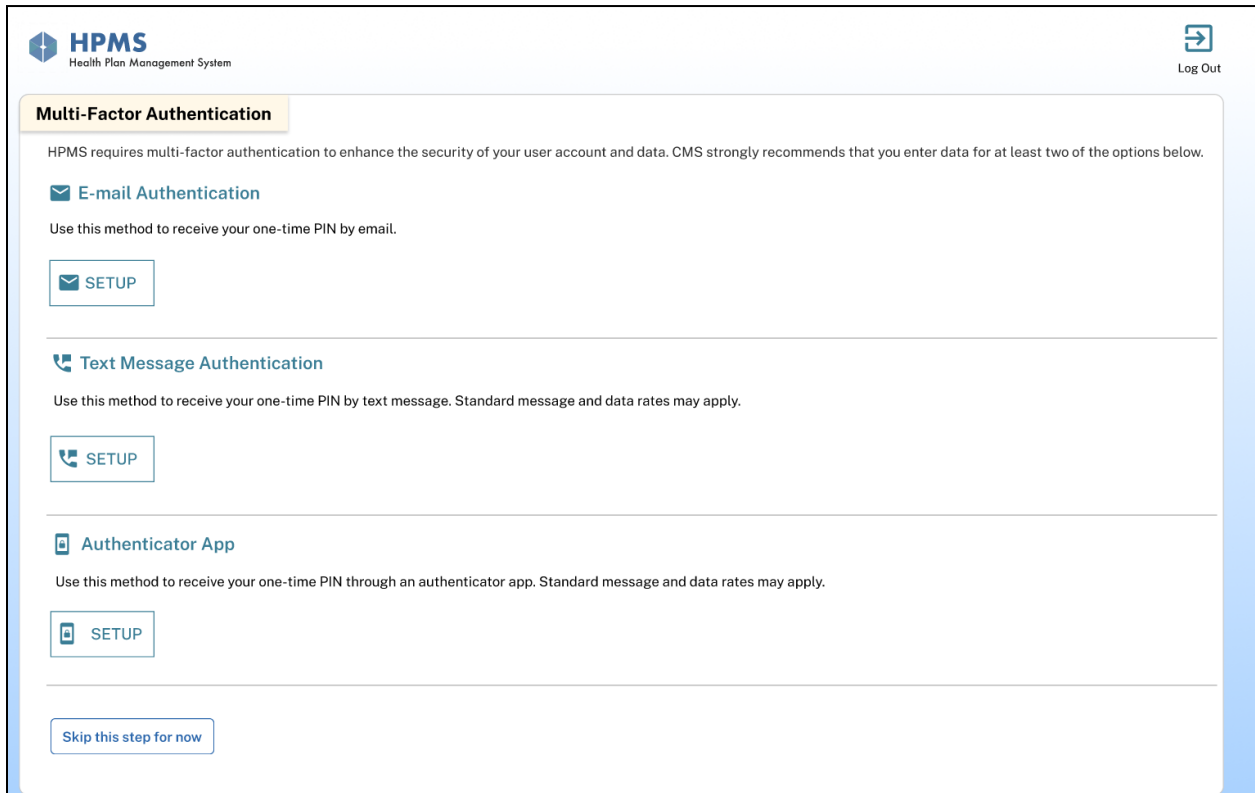


Figure 2: HPMS MFA Initial Set Up Page

4. You must click on the **Setup** button for one or more of the three options above to establish your MFA factors.
- A 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.
 - 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.
 - 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. These questions will be used if you are unable to log into HPMS using MFA and need to reset your account.

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

Figure 3: HPMS Security Questions Page

6. You will be sent to the HPMS home page after completing the security questions.

LOGGING IN AFTER SETTING UP MFA

1. Log into HPMS from the HPMS landing page using your CMS EUA user ID and password.
2. Select the method to receive your one-time PIN (OTP).

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.

Figure 4 : Select Method to Receive OTP Page

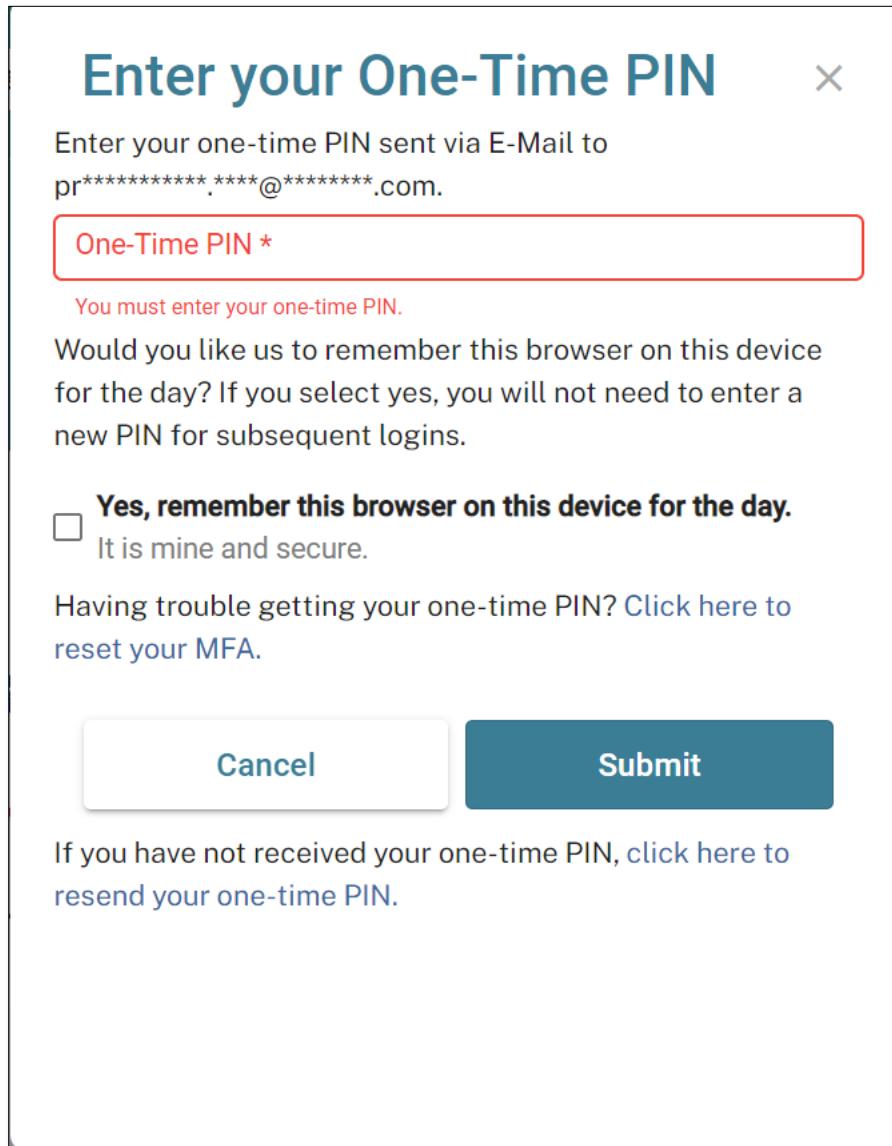
3. Enter your OTP on the following page. You also have the option to remember the OTP on the specific browser on your device for the remainder of the day.

Figure 5: Enter your OTP Page.

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

RESETTING THE MFA

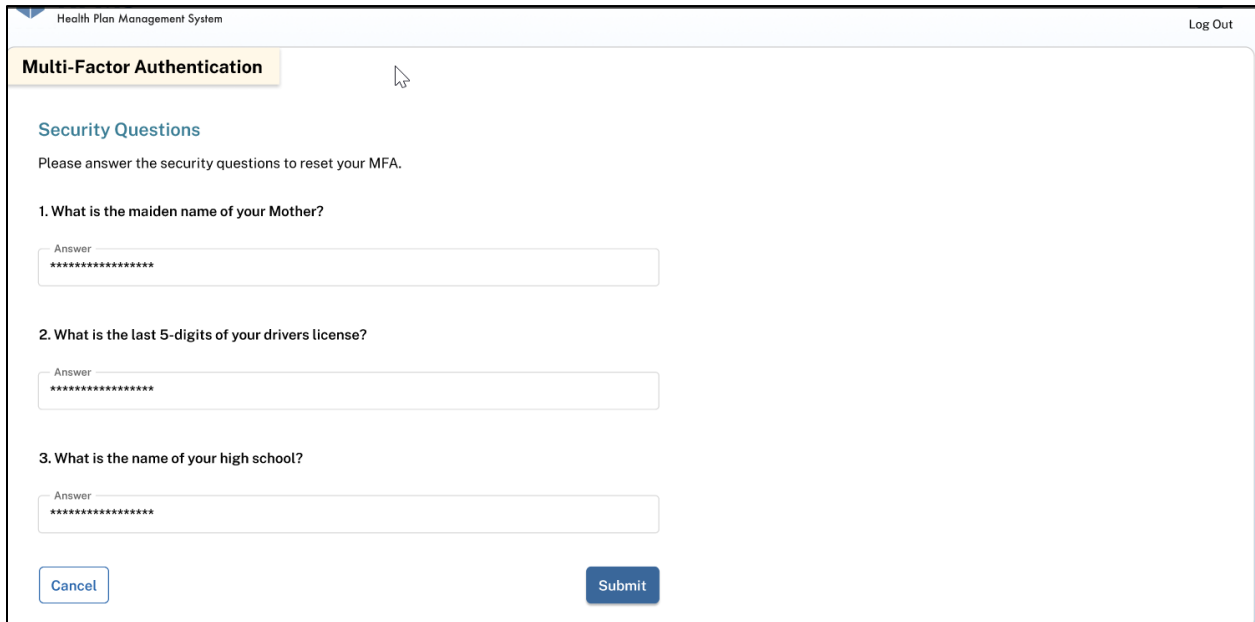
1. If you are unable to complete MFA successfully, use the **Click here to reset your MFA** link.



The screenshot shows a modal dialog box titled "Enter your One-Time PIN" with a close button (X) in the top right corner. The text inside the dialog 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." This is followed by a checkbox and the text: "Yes, remember this browser on this device for the day. It is mine and secure." Below the checkbox is a link: "Having trouble getting your one-time PIN? Click here to reset your MFA." At the bottom of the dialog are two buttons: "Cancel" (white with a grey border) and "Submit" (solid teal). 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."

Figure 6: Reset your MFA link

2. You will be directed to complete your HPMS security questions.



The screenshot shows a web browser window titled "Health Plan Management System" with a "Log Out" link in the top right corner. The main content area is titled "Multi-Factor Authentication" and contains a section for "Security Questions". Below this section, there is a prompt: "Please answer the security questions to reset your MFA." Three numbered questions are listed, each followed by an "Answer" label and a text input field containing asterisks. The questions are: 1. "What is the maiden name of your Mother?", 2. "What is the last 5-digits of your drivers license?", and 3. "What is the name of your high school?". At the bottom of the form, there are two buttons: "Cancel" on the left and "Submit" on the right.

Figure 7: Modify HPMS Security Questions Page

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 **Please click here** link on the Multi-Factor Authentication tab.

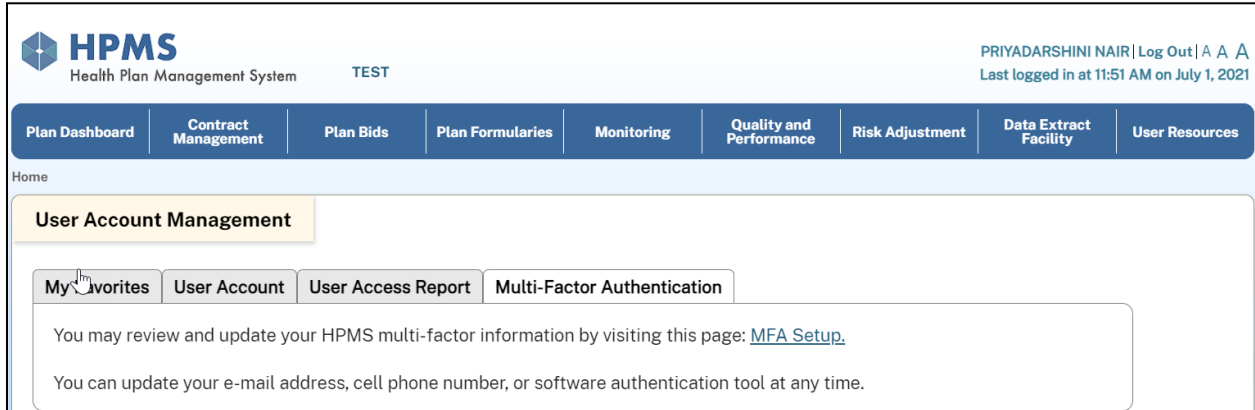


Figure 8: HPMS User Account Management Page

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

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: *****

Figure 9: HPMS MFA Method Update Page