



CENTER FOR MEDICARE

DATE: July 9, 2021

TO: All HPMS Users

FROM: Amy Larrick Chavez-Valdez, Director
Medicare Drug Benefit and C & D Data Group

SUBJECT: Follow-Up on Multi-Factor Authentication for the Health Plan Management System

As announced in a February 9, 2021 memorandum, CMS is implementing a multi-factor authentication solution for the Health Plan Management System (HPMS). This change is required to adhere to federal system security mandates.

Multi-factor authentication (MFA) is a mechanism that requires two independent user credentials to access a system (i.e., a CMS password and a second token that only the user could possess). Users may have experience with MFA when accessing other sensitive websites, such as using a code sent by text message to a personal device in order to log into a bank account.

CMS is offering a pilot window so that users can configure MFA settings and reset questions and start to log into HPMS using your MFA credentials. The pilot window will begin on **Monday, July 19, 2021 and run through Sunday, August 15, 2021**. During this time, users will be prompted to set up MFA credentials with step-by-step on screen instructions. Please note that users may also choose to bypass the setup process during the pilot window via the “Skip this Step” option.

On Monday, August 16, 2021, MFA will be mandatory in order to log into HPMS. As a result, CMS strongly recommends that HPMS users take advantage of the pilot window to setup and test the new MFA login to ensure continued access to HPMS on August 16, 2021.

HPMS will provide the following second factor options for users that log into the system from *outside* the CMS network:

1. **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.
2. **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.

3. **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 first two delivery mechanisms.

Please see **Appendix A** for an HPMS MFA quick reference guide.

Important Note: CMS users will only be required to use the second token when accessing HPMS from outside of the CMS network (e.g., from a personal device).

Please direct questions regarding HPMS MFA to the HPMS Help Desk at either hpms@cms.hhs.gov or 1-800-220-2028.