Preclusion List – EIDM to IDM Migration – Help Guide

The Centers for Medicare & Medicaid Services (CMS) will migrate the EIDM system to CMS Identity Management (IDM) system on Friday, February 19, 2021, with the first date end users will encounter IDM as Monday, February 22nd. The Preclusion List application uses EIDM (and in future IDM) for Identity and Access management. The purpose of this document is to provide the existing Preclusion List users with necessary information about the IDM system and highlight a few key differences between the two systems.

Important IDM Information:

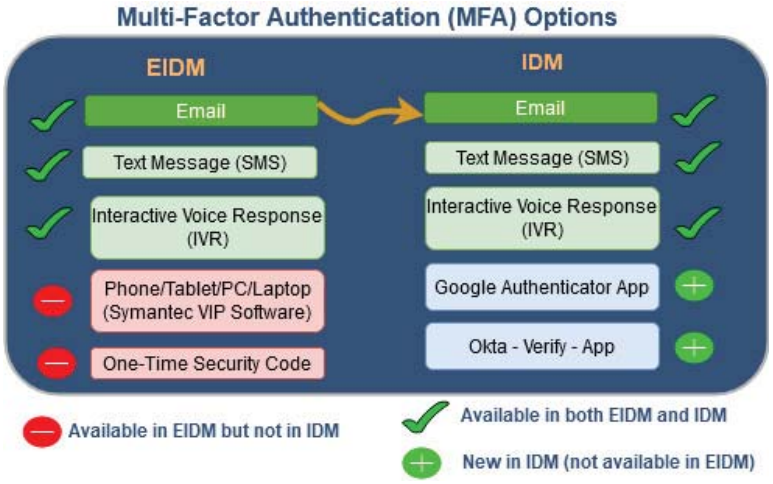
1. Users will continue to login to the CMS portal (https://portal.cms.gov/) to access the IDM system.

2. Information that will be migrated from EIDM to IDM:
   - User Profile – User ID, Password, and basic profile information such as Name, Email, DOB, SSN, Addresses, etc.
   - Role Information – Existing Preclusion List application role will be migrated.
   - Account Security Questions – Only one security question & answer will be migrated to the IDM system and it will be a random pick. Please ensure you have the answer to all security questions under the existing EIDM system.

3. **Multi-Factor Authentication**: For all current Preclusion List users, the default Multi-Factor Authentication (MFA) available initially is Email. Once a user is able to login into the IDM system, additional MFA devices can be registered.

Below figure shows the comparison of available MFA options between the EIDM and the IDM systems:

Figure 1 - MFA Options - EIDM vs. IDM



- Symantec VIP software and one-time security code options are no longer available in the IDM. Instead, Google Authenticator and Okta Verify mobile apps are available as new MFA options.
- Google Authenticator App – Can be downloaded from the Google Play Store. PC-based users of the Google Chrome browser can install and use Authenticator Extension to register as an MFA device instead of a Phone app.
- Okta Verify – This mobile app can be downloaded from the Google or Apple app stores. Okta Verify mobile app uses Push approval instead of entering the 6-digit security code.

4. Suggested Next Actions:

- Login to EIDM / CMS Portal (https://portal.cms.gov) and ensure that the profile Email is valid and accessible to receive the security code.
- Please make sure that you have answers to the EIDM security questions, which will be needed to perform self-service functions such as account unlock / password reset.
- You may log in to the IDM system but do not make any changes to the profile information until the final transition notification is sent to you.
- Any additional MFA devices such as SMS, IVR, Symantec VIP software, etc. in EIDM will not be migrated to IDM and will need to be re-registered

Please Note: Users can log into PROD and perform profile updates prior to 2/19. Users can add MFA devices, update SQA, etc. However, please do not remove or add any roles in PROD before the February 22, 2021.

5. Helpdesk Support and Questions:

- Under the new IDM system, the Helpdesk cannot provide one-time security code. They can only update an Email, which can then be used to request the MFA security code.
- For all account issues related to EIDM (or IDM, after the migration), please contact the EUS helpdesk using one of the following options:
  - Email: EUSSupport@cgi.com
  - Live chat: https://eus.custhelp.com/
  - Phone: (866) 484-8049 + option #1 + Option #2 between 7am – 7pm EST, Monday – Friday.

- For questions related to Preclusion List or Preclusion List data, send an email to PreclusionList@cms.hhs.gov.