ACO-MS
TIP SHEET

MEDICARE
SHARED SAVINGS
PROGRAM

ACO-MS: Access Information

Version 6 | March 2023

OVERVIEW

- The purpose of this document is to provide information on how to obtain access to the ACO Management System (ACO-MS) and what to expect the first time you sign into the system. View the Contact Us/FAQ page in ACO-MS for additional information.

HOW TO INVITE USERS TO ACO-MS

- ACO users with administrative privileges (ACO Executive, CMS Liaison, Authorized to Sign Contacts (primary and secondary), or Application Contacts (primary and secondary)) can invite others to join ACO-MS. To invite a new user, log into ACO-MS, navigate to the My ACOs tab, and select your ACO. On the next page, click on the Contacts subtab.
- The Contacts subtab displays all users currently associated with your ACO. To add a new user, select the "Add New Contact" button, enter the individual's name, contact type, email address, and business address. Next, click "Send Invite" and the system will send that individual an email invitation.

INVITED USERS

- Invited users will receive an email invitation that includes a link that will be valid for 15 days and a security code to initiate the account setup process. This process varies depending on whether the invited user already has an Identity Management (IDM) ID. If an invited user does not establish an ACO-MS account within 15 days of receiving the invitation, the invitation will expire, and a new invitation must be generated.

Account Registration for Invited Users with an IDM ID

- After clicking the link in the email invitation, the invited user should select "Yes" to confirm they have an IDM ID.
- The user will be directed to a sign-in page and will enter their IDM ID and IDM password.

Account Registration for Invited Users without an IDM ID

- After clicking the link in the email invitation, the invited user should select "No" to confirm that the user does NOT have an IDM ID.
- The user will enter personal information, including their legal name, email, and phone number; choose a user ID and password; and select and answer a challenge question to enable password reset as part of the account registration process.
- Once registration is complete, the user will sign back into ACO-MS using the newly created user ID and password to activate their account.

REMOTE IDENTITY PROOFING

- Remote Identity Proofing (RIDP) is the process of validating personal information (e.g., credit history, personal demographic information, and other indicators) to confirm one's identity.
- CMS uses the Experian identity verification service, which generates a list of questions based on the user's legal name, current residential address, phone number, and Social Security number.
- A user without an IDM ID will need to complete RIDP before accessing ACO-MS. RIDP only needs to be completed one time. A user that already has an IDM ID does not need to complete this step.
- If you encounter an error, you will receive an error message that includes an Experian Reference number to use when contacting the Experian help desk at 1-866-578-5409.

MULTI-FACTOR AUTHENTICATION

- ACO-MS requires Multi-factor Authentication (MFA). MFA adds an additional layer of security and requires that a user enter a security code sent via email, text, or phone call in addition to a username and password each time they sign into the system. Setting up MFA using phone call or text is recommended.
- A user with an IDM ID can use the MFA device already associated with their IDM ID and does not need to complete this step.
    - Users with existing EIDM accounts who are migrated to the new IDM solution will have their MFA code delivery method defaulted to the email address associated with their EIDM account. Once the user accesses ACO-MS for the first time after the migration, they will be able to add additional MFA methods, such as phone call or text.
- All other users will need to set up MFA when they sign into ACO-MS for the first time. By default, the MFA code will be delivered to the email provided during the account registration process. Users can add additional MFA methods, such as phone call or text.
- All users may change their default MFA authentication delivery method when logging in by clicking the dropdown arrow and selecting their preferred authentication factor.

Questions?

If you have any questions about ACO-MS or require technical assistance, click the SSP Helpdesk icon (located within the ACO-MS banner) or email SharedSavingsProgram@cms.hhs.gov.

If you have any questions regarding RIDP, contact the Experian help desk at 1-866-578-5409.