ACO-MS How to

MEDICARE SHARED SAVINGS PROGRAM

How to Manage ACO-MS User Access & Contacts

Version 1 | March 2024

An ACO has the ability to manage its organization's user access and contact types in the ACO Management System (ACO-MS). CMS encourages ACOs to regularly review their users' access and update their contacts accordingly. This document provides definitions of the various ACO contact types and the permissions associated with those types in ACO-MS.

⚠ Important

- An individual can serve as more than one type of contact. However, CMS recommends you diversify your contacts by identifying multiple people to serve as ACO contacts.
- Please be mindful that primary and secondary contacts must be two different people.
- Please update the Contact Data page in ACO-MS with the appropriate contact information when there is a change in ACO contacts within your ACO (e.g., new personnel, departing personnel, changes in roles).
- ACOs can have more than one person designated as secondary contact(s). For example, having more than one person that can sign documents on behalf of your ACO (i.e., Authorized to Sign secondary contact) may save individuals' time when executing ACO Participant Agreements or completing the yearly ACO Signing Event.

User Access and Contact Management Resources

All individuals requiring access to an ACO must be invited to ACO-MS by an ACO contact with administrative privileges (ACO Executive, CMS Liaison, Authorized to Sign Contacts (primary and secondary), or Application Contacts (primary and secondary)).

ACO users with administrative privileges may add new users to their organization by following these steps:

1. Log into ACO-MS and navigate to the My ACOs tab on the left side menu.
2. Select your ACO.
3. Go to the Contacts subtab, which displays all users currently associated with your ACO.
4. Select "Add New Contact."

   Complete the required fields. The system will then send an email invitation to the invited user.

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. 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. This process varies depending on whether the invited user already has an Identity Management (IDM) ID.

Account Registration for Invited Users with an IDM ID

1. After clicking the link in the email invitation, the invited user should select “Yes” to confirm they have an IDM ID.
2. 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

1. 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.
2. 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.
3. 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 used to confirm one’s identity. For ACO-MS, CMS employs the Experian identity verification service, which uses questions based on personally identifiable information to verify identity. This process is conducted online but may be conducted via telephone or with the assistance of the SSP Help Desk if the user is unable to complete it online.
    - A user without an IDM ID will need to complete RIDP before accessing ACO-MS. RIDP only needs to be completed once. 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 1-833-985-0709.

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 Enterprise Identity Managemnet (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 users who do not currently have an IDM ID 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.

CONTACT CAPABILITIES

	This contact has administrative privileges in ACO-MS they can edit or delete invited ACO users.	This contact can be the same as the Authorized to Sign (primary or secondary) Contact or the ACO Executive Contact.	This contact is designated to electronically sign documents on behalf of the ACO.	This contact has access to correspondence from CMS to the ACO.
Required Contacts				
ACO Executive	X	X	X	X
Applicant Contact (primary)	X			X
Authorized to Sign (primary and secondary)	X	X	X	X
CMS Liaison	X			X
Compliance Contact				X
DUA Custodian				X
DUA Requestor			X	X
Financial Contact				X
Information Technology (IT) Contact (primary)				X
Marketing Contact (primary and secondary)				X
Medical Director				X
Primary Contact (Public Usage)*				X

	This contact has administrative privileges in ACO-MS they can edit or delete invited ACO users.	This contact can be the same as the Authorized to Sign (primary or secondary) Contact or the ACO Executive Contact.	This contact is designated to electronically sign documents on behalf of the ACO.	This contact has access to correspondence from CMS to the ACO.
Quality Contact (primary and secondary)				**X**
Optional Contacts				
Application Contact	**X**			**X**
IT Contact (secondary)				**X**

*CMS may share this Primary Contact (Public Usage) with other Accountable Care Organizations to resolve overlaps.

CONTACT DESCRIPTIONS

Required ACO Contacts

ACO Executive: Person who holds an executive leadership office in the ACO and is vested by the ACO's governing body with the legal powers to commit the ACO to a binding agreement.

Application Contact (primary): Serves as the primary point of contact for the ACO's application to participate in the Medicare Shared Savings Program (Shared Savings Program).

Authorized to Sign (primary): Person appointed by the ACO as an agent of the organization and vested by the ACO's governing body with the legal powers to commit the ACO to a binding agreement.

Authorized to Sign (secondary): Person appointed by the ACO as an agent of the organization and vested by the ACO's governing body with the legal powers to commit the ACO to a binding agreement.

CMS Liaison: Serves as the ACO's point of contact for communication between the ACO and CMS.

Compliance Contact: Serves as the ACO's point of contact for program compliance and monitoring activities. This includes compliance and monitoring activities, such as corrective action plans (CAPs) and program announcements and notices related to compliance and monitoring.

DUA Custodian: Individual responsible for the observance of all conditions of data use and for establishment and maintenance of security arrangements, as specified in the DUA, to prevent unauthorized use or disclosure. The custodian is the individual who accesses the requested data files and oversees others within the organization who have access to it. All ACO contacts listed in ACO-MS are considered DUA Custodians.

DUA Requestor: Serves as the person authorized to legally bind the ACO to the terms of the DUA. Each ACO can only have one DUA Requestor.

Financial Contact: Serves as the ACO's point of contact for banking and payment information. This person is the ACO's authorized official recorded on the ACO's Form CMS-588 and owner of the ACO's bank account.

Information Technology (IT) Contact (primary): Serves as the ACO's primary point of contact for data transfers between the ACO and CMS.

Marketing Contact (primary): Serves as the ACO's primary point of contact for marketing materials and activities provided on behalf of the ACO.

Marketing Contact (secondary): Serves as the ACO's secondary point of contact for marketing materials and activities provided on behalf of the ACO.

Medical Director: This senior-level position is held by a board-certified physician who is licensed in the state where an ACO operates and is physically present on a regular basis at any clinic, office, or other location of the ACO, an ACO participant, or an ACO provider/supplier. This person provides leadership and oversight of the ACO's clinical management and is familiar with the ACO's organizational culture and day-to-day operations.

Primary Contact: Serves as the ACO's point of contact for the public about the ACO. This person must be accessible by phone or email.

Quality Contact (primary): Serves as the ACO's primary point of contact for Shared Savings Program quality activities.

Quality Contact (secondary): Serves as the ACO's secondary point of contact for Shared Savings Program quality activities.

Optional ACO Contacts

Although not required, CMS recommends that ACOs designate individuals to all optional contacts.

Application Contact (secondary): Serves as the secondary point of contact for the ACO's application to participate in the Shared Savings Program.

IT Contact (secondary): Serves as the ACO's secondary point of contact for data transfers between the ACO and CMS.

Other Contact: One or more individuals supporting the ACO who do not have any of the responsibilities described in the contact definitions above.

Quality Related Contacts Descriptions

API Credentials Contact

Credential Delegate: Is used exclusively to access the Application Programming Interface (API) environment.

- This person has full read access in ACO-MS; however, they cannot edit information outside of the API Credentials Management Module.

- This role can only be added by the ACO Executive, Authorized to Sign Contact (primary or secondary), CMS Liason, or Application Contacts (primary and secondary).

Quality Payment Program (QPP) Contacts

- This person has view access to the ACO Signing Event, Change Request, Reporting, Data Hub, and Knowledge Library tabs in ACO-MS.

Quality Payment Program (QPP) Security Official (optional): Performs all of the functions of a QPP Staff User, plus approves or denies requests from other users requesting access to your organization in the QPP website. Each ACO must have at least one individual with the QPP Security Official role.

QPP Staff User (optional): Accesses the QPP website in order to submit the quality measures data required under the Shared Savings Program.

- This person has access to the ACO's Merit-based Incentive Payment System (MIPS) performance feedback and can request a targeted review.

Additional individuals who need access to the QPP website may be invited to obtain the QPP Security Official or QPP Staff User role. For a full list of functions that users with the QPP roles can perform in the QPP website, refer to the *Creating and Managing Quality Payment Program Contacts in ACO-MS* tip sheet available in the Program Resources section of the Knowledge Library tab in ACO-MS.

Note: All individuals who need a Health Care Quality Information System (HCQIS) Access Roles and Profile (HARP) account with a QPP Security Official or QPP Staff User role should contact one of their ACO contacts with administrative privileges to request an invitation to obtain a QPP role and manage their QPP roles in ACO-MS. Individuals should not create HARP accounts or manage their QPP roles via the QPP website. For more information, please refer to the Quality Payment Program Access User Guide zip file.

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.