ACO-MS
TIP SHEET

MEDICARE
SHARED SAVINGS
PROGRAM

Overview of ACO-MS User Access and ACO Contacts

Version 7 | November 2023

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."
5. Complete the required fields. The system will then send an email invitation to the invited user that includes a link and security code, which will be valid for 15 days, to initiate the account setup process.*

   During the account set-up process, new users **without an Identity Management (IDM) ID will be prompted to complete a series of remote identity proofing (RIDP) questions. RIDP requires the user to verify personal information (e.g., personal demographic information) to confirm one's identity. New users will also need to set up multi-factor authentication (MFA) when they sign into ACO-MS for the first time.*

ACO users with administrative privileges can also update their ACO's existing contacts. The user's role will be updated automatically, and they will be assigned any corresponding permissions. If an ACO contact needs to update their contact information in ACO-MS, an ACO User with administrative privileges will need to send a new invite to the new email. Once the invite is received and activated, the ACO should terminate the old contact information in ACO-MS.

An ACO user **with** an existing IDM ID can accept a contact invitation in one of two ways:

1. Log into ACO-MS and review the Activation Widget on the Dashboard to check if they have any pending ACO-MS contact invitations. The user can then select either "Activate" or "Decline Request." All activated contact roles will display in the Contacts subtab.
2. Access the email invitation, select the email link to ACO-MS, and use the provided security code to sign into the system.

An ACO user **without** an existing IDM ID can accept a contact invitation by accessing the email invitation, selecting the email link to ACO-MS, and using the provided security code to sign into the system.

For additional support regarding signing into ACO-MS, refer to *ACO-MS: Initial Access Information*.

REQUIRED ACO CONTACTS

*** Indicates ACO Contact has administrative privileges in ACO-MS.*

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.

- *This person may or may not be the same as the Authorized to Sign (primary or secondary) Contact.*
- *This person receives and has access to correspondence from CMS to the ACO.*
- *This is a required contact type for the ACO Signing Event; this role is designated to electronically sign documents on behalf of the ACO.*
- *This person can edit or delete invited ACO users.*

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.

- *This person may or may not be the same as the ACO Executive Contact.*
- *This person receives and has access to correspondence from CMS to the ACO.*
- *This is a required contact type for the ACO Signing Event; this role is designated to electronically sign documents on behalf of the ACO.*
- *This person can edit or delete invited ACO users.*

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.

- *This person may or may not be the same as the ACO Executive Contact.*

- *This person receives and has access to correspondence from CMS to the ACO.*
- *This is a required contact type for the ACO Signing Event; this role is designated to electronically sign documents on behalf of the ACO.*
- *This person can edit or delete invited ACO users.*

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.

- *This is a required contact type for the ACO Signing Event; this role is designated to electronically sign the DUA on behalf of the ACO.*

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.

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

- *This person receives and has access to correspondence from CMS to the ACO.*
- *This person can edit or delete invited ACO users.*

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).

- *This person receives and has access to correspondence from CMS to the ACO.*
- *This person can edit or delete invited ACO users.*

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

- *This person receives and has access to correspondence from CMS to the ACO.*

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.

- *This person receives and has access to correspondence from CMS to 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.*

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.*
- *This person receives and has access to correspondence from CMS to the ACO.*

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

- *This person receives and has access to correspondence from CMS to the ACO.*

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

- *This person receives and has access to correspondence from CMS to the ACO.*

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

- *This person receives and has access to correspondence from CMS to 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.

- *This person receives and has access to correspondence from CMS to the ACO.*

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

- *This person receives and has access to correspondence from CMS to the ACO.*

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.

- *This person receives and has access to correspondence from CMS to the ACO.*
- *This person can edit or delete invited ACO users.*

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

- *This person receives and has access to correspondence from CMS to the ACO.*

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

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 or an Authorized to Sign Contact (primary or secondary*).

QPP CONTACTS

QPP Security Official (required): 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.

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

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: Beginning August 5, 2021, 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.

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.