DEPARTMENT OF HEALTH & HUMAN
SERVICES
Centers for Medicare & Medicaid Services 7500
Security Boulevard
Baltimore, Maryland 21244-1850

CENTER FOR MEDICARE

DATE: October 31, 2025

TO: All Medicare Advantage Organizations, Prescription Drug Plans, Cost Plans, PACE Organizations, and Demonstrations

FROM: Jennifer R. Shapiro, Director, Medicare Plan Payment Group

SUBJECT: Annual Designation of Identity Management (IDM) Plan's User Approver/External Point of Contact (EPOC) - ACTION

The purpose of this letter is to remind Medicare Advantage Organizations (MAO) and Prescription Drug Plan (PDP) sponsors of the requirements and processes that must be utilized annually to designate staff the responsibility as the plan's External Point of Contact (EPOC) for purposes of granting access to beneficiary and contract level eligibility/enrollment, payment, and premium data in CMS systems. Furthermore, this letter provides an overview of the procedure a plan's EPOC should use to conduct the annual certification for existing end users' access.

CMS security policies require separation of duties between system administrators and users. In particular, the policy addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions.

Separation of duties aligns privileges with appropriate roles with the idea that specific duties are distinctly different from one another to reduce the risk of malevolent or inappropriate behaviors based on access. Implementing this control helps reduce the risk of inappropriate access to Personally Identifiable Information (PII) or Personal Health Information (PHI) (e.g., separating employees that perform security investigations from mission and business functions).

Separation of duties regarding a plan's EPOC is implemented by designating a selected set of administrators from the MAO/PDP and rendering them the capability to set permissions for their company's employees and /or First Tier Downstream Entities when accessing PII and PHI from CMS systems.

Identity Management (IDM) is the Internet-accessible application where an organization's employee will register to become a plan's EPOC for their company's end users who may want access to the CMS Medicare Advantage Prescription Drug System (MARx).

Rules of Behavior and Responsibilities of the Plan's EPOC

CMS is committed to maintaining the integrity and security of health care data in accordance with applicable laws and regulations. Provisions of the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act (HIPAA) of 1996 places restrictions on the disclosure of Medicare eligibility, enrollment, premium, premium withhold, and payment data. The plan's EPOC is an employed representative of a MAO or PDP whose responsibility is to approve/reject, maintain, manage, and certify their company's employees' and /or First Tier Downstream Entities access to MARx. The plan's EPOC will not be able to obtain access to MARx, however. All users granted access by the plan's EPOC shall use Medicare beneficiary data for conducting Medicare business only.

More information on the Rules of Behavior regarding a plan's EPOC can be found on the CMS.gov webpage:
https://www.cms.gov/research-statistics-data-and-systems/cms-information-technology/mapdhelpdesk/plan-connectivity-preparation

The Registration Process for the Plan's EPOC

CMS requires organizations to annually select a qualified official as their plan's EPOC, such as a manager, supervisor of Information Technology, or a Systems Security Officer. After providing the preliminary information to CMS, the plan's EPOC utilizes IDM to assign themselves as the steward of the appropriate contract number(s) as part of completing the registration process.

When CMS approves a registration request, the plan's EPOC is then able to approve/reject their company's end user request to access the CMS systems. The following steps must be completed to designate a plan's EPOC:

Step One – Email the EPOC Designation Letter to CMS

The plan must email an official company letter to CMS identifying and appointing the plan's EPOC. Please note that an organization may submit one letter for all contract numbers and may designate up to two plan EPOCs for the same (or different) contract numbers for their organization. Any special requests for adding more than two plan EPOCs are reviewed on a case-by-case basis.

The EPOC Designation Letter must:

- be on letterhead
- contain all of the following information for each plan's EPOC:
  - Name(s) of designated plan EPOC
  - Mailing address
  - Telephone number and extension
  - E-mail address
  - Contract number(s) for which the plan's EPOC will approve users (list ALL contract numbers in **alphanumeric order**)

- contain a signature of a senior official within the organization (i.e. CEO, CIO, CFO, or COO since the individual signing the letter cannot be a plan's EPOC); include the name, title, mailing address, e- mail address, and telephone number of the company official signing the letter.

In addition to the letter, the plan must fill out and email a signed EPOC Access Acknowledgement Form. The template for the EPOC Designation Letter and EPOC Access Acknowledgement Form is in the Plan Connectivity Preparation section of the MAPD Help Desk website.

The EPOC Designation Letter and EPOC Access Acknowledgement Form for each individual plan's EPOC should be:

- Emailed as a separate email to DPOEPOCS@cms.hhs.gov and copy mapdhelp@cms.hhs.gov
- The email subject line must follow the format below:
    - The plan EPOC's Name (must match the name used to register in IDM – no nicknames)
    - Company Name
    - Contract Number(s) – if registering for more than 1, please only enter 1 contract number in subject line
    - Example: Subject: Jane Doe, Company Name, HXXXX

Step Two – Complete registration in IDM

- URL – https://portal.cms.gov
- The plan's EPOC should select the EPOC role under the MARx application. The Plan Connectivity Preparation section of the MAPD Help Desk website provides a registration walk through document in the downloads section.
- During the registration process, potential plan EPOC users should provide all contract numbers for which they will approve end users (they may add additional contracts later).
- Enter an e-mail account address that is specific to their organization (not a publicly available e-mail account such as Gmail or Hotmail).
- The name used on the EPOC Designation Letter must match the name used to register in IDM.
- Enter a valid phone number and extension. This information is necessary in case an issue arises and CMS must contact a potential plan EPOC directly.

Step Three – Confirm receipt of CMS approval

- CMS will not approve access until the plan has completed steps one and two.
- Once CMS approves the registration, the newly appointed plan EPOC will receive an e-mail from IDM confirming access granted. Once an email is received, the new plan EPOC can begin to approve their company's access requests.
  *If there is no email response received, the potential plan EPOC should make sure to check spam folders for the email.

Any subsequent changes, additions, or deletions to a plan's EPOC designation require the plan to follow the instructions outlined above and provide CMS with a new letter that clearly identifies the changes and/or deletions. The plan's EPOC will be able to register or add/delete contracts to their registration in IDM.

The MAPD Help Desk also manages the deletion of plan EPOCs that no longer need access, however a plan's EPOC should first attempt to remove all contracts from their role before contacting the MAPD Help Desk. The MAPD Help Desk can be reached at 1-800-927-8069 or mapdhelp@cms.hhs.gov.

Annual IDM Role Certification for the Plan's EPOC

CMS requires an annual submission of the EPOC Designation Letter and EPOC Access Acknowledgement Form before approving the plan's EPOC annual IDM role certification. The documentation will be used by CMS to verify and approve new or existing plan EPOC designations. EPOC Designation Letters and EPOC Access Acknowledgement Forms should be emailed to DPOEPOCS@cms.hhs.gov. **The deadline for submitting the letter to CMS is December 1st each year.** CMS will not approve a plan's EPOC certification if the information is not submitted timely and will result in the removal of a plan's EPOC role.

Annual IDM Role Certification for Plan Users

A plan's EPOC is required to establish a procedure for maintaining plan user access under their authority. CMS recommends a user review occur twice a year, as well as the annual IDM role certification. Annual IDM role certification is the process by which a plan's IDM user attests to and is verified by the plan's EPOC for continued use of an IDM role prospectively for 365 days. Annual role certification is required every year by CMS' security policy and is counted from the original role approval date or the previous year's certification date.

More information on performing the role certification in IDM can be found on the CMS.gov webpage:
https://identity.cms.gov/store/idm_documentation#userGuides

Note: If a plan's EPOC chooses to bulk approve plan user access during the certification process, the plan's EPOC is verifying they have thoroughly reviewed the access on each user and that access is still required and appropriate. CMS continues to perform reviews to ensure proper processing.

If you have any questions or concerns about any of the information within this letter or wish to inquire about the annual designation of a plan's EPOC, please contact the MAPD Help Desk at mapdhelp@cms.hhs.gov, or 1-800-927-8069.