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

DATE: September 2, 2021

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

FROM: Jennifer R. Shapiro, Medicare Plan Payment Group

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

This letter describes the requirements and process that Medicare Advantage Organizations (MAO) and Prescription Drug Plans (PDP) must use to designate staff that will be responsible for granting access to data in the CMS systems, as well as the responsibilities of a MAO/PDP CMS External Point of Contact (EPOC). Furthermore, this letter provides an overview of the procedure in which an EPOC should conduct the annual certification for existing end users' access.

Identity Management (IDM) is an Internet-accessible application that will allow an organization's employee the ability to register for access to the CMS Medicare Advantage Prescription Drug (MAPD) systems or become a designated approver for their company's end users. **The EPOC's role is to approve other employees' access, while they themselves cannot register to access the CMS Medicare Advantage/Prescription Drug system.**

The CMS Acceptable Risks and Safeguards (ARS) 3.1 security policy for Access Control-05 (AC-05) requires separation of duties between system administrators and users. AC-05 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 duties are split between roles in such a way as 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) (e.g., separating employees that perform security investigations from mission and business functions).

Separation of duties is implemented by designating a selected set of administrators the capability to set user permissions to access PII and Protected Health Information (PHI), while those

administrators do not themselves have access to the PII and PHI. The principle of separation of duties is significant for developers as well as for operational system administrators.

EPOC Registration Process

CMS recommends that organizations select a qualified official, such as a manager or supervisor of the IT or Security department, to be the EPOC. After providing the preliminary information to CMS, each EPOC registers for the appropriate contract numbers using IDM. When CMS approves a request, the EPOC is able to approve or reject their company's employee and subcontractors' access to CMS systems. The following steps must be complete in order to designate an EPOC:

Step One – Email EPOC designation letter to CMS

CMS no longer accepts EPOC designation letters via mail. The plan must email an official company letter to CMS identifying and appointing the EPOC. Please note that an organization may submit one letter for all contract numbers and may designate up to two EPOCs for the same (or different) contract numbers for your organization. Any special requests for adding more than two EPOCs are on a case-by-case basis.

The EPOC designation letter must:

- be on original letterhead;
- contain all of the following information for each EPOC:
    - Name(s) of designated EPOC
    - Mailing address
    - Telephone number and extension
    - E-mail address
    - Contract number(s) for which the EPOC will approve users (list ALL contract numbers under which this EPOC will approve users to work)
- contain a signature of the responsible officer of the organization;
- 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 should be:

- Emailed to DPOEPOCS@cms.hhs.gov and copy MAPDHELP@cms.hhs.gov;
- The email subject line must follow the format below:
    - EPOC 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
- During the registration process, potential EPOC users should provide all of the 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 Yahoo 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 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 EPOC will receive an e-mail from IDM confirming access granted. Once an email is received, the new EPOC can begin to approve its company's access requests.
  *If there is no email response received, the potential 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 EPOC will be able to register or add/delete contracts to their registration in IDM.

The MAPD Help Desk also manages the deletion of EPOCs that no longer need access, however an EPOC should first attempt to remove all contracts from his/her 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 Certification

A plan's EPOC is required to establish a procedure for maintaining plan user access under their authority. A user review should occur twice a year, as well as an annual recertification. EPOCs are required to certify their company's end users annually. An extension will not be granted to EPOCs who do not comply with the annual recertification timeframe since this is considered a CMS security violation. If an EPOC chooses to bulk approve plan users during the certification process, the 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.

Due to the frequent changes in EPOC assignments and annual certification of all users, an annual submission of an EPOC Designation Letter and EPOC Access Acknowledgement Form is required. EPOC Designation Letters and EPOC Access Acknowledgement Forms can be emailed to DPOEPOCS@cms.hhs.gov. **The deadline for submitting the letter to CMS is December 1st each year.** CMS will not approve EPOC certification if this information is not submitted and/or the EPOC does not initiate a request for annual certification.

EPOCs are required to keep their accounts active and current, and failure to access the IDM system within a 60-day period will suspend their account. CMS has the authority to remove access from any EPOC whose account is in a suspended status, and the user must complete the EPOC registration process again.

Instructions regarding EPOC and end user registration are documented in the Data Exchange Preparation Procedures (DEPP) located at:
https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/mapdhelpdesk/Plan-Connectivity-Preparation

Please direct any questions to the MAPD Help Desk at 1-800-927-8069 or MAPDHELP@cms.hhs.gov.