Division of Payment Operations (DPO)

Medicare Advantage / Part D Maintenance Program (MAPD)

External Point of Contact (EPOC) Rules of Behavior (ROB)

For Granting Access to the Medicare Advantage Prescription Drug System (MARx)

FINAL

Version/Date: V1.0 / May 16, 2023

Table of Contents

1 External Point of Contact (EPOC) Rules of Behavior 3
1.1 Providing MARx Access: EPOC Responsibilities 4
1.2 Authorized Roles to Access MARx 6
1.3 Authorized Purposes for Accessing MARx 8
1.4 Unauthorized Purposes for Accessing MARx 8

Revision Log

Date	Version No.	Description	Analyst
4/29/2023	1.0	Significant design of document including content, formatting, and grammatical corrections	CMS DPO ISSO
4/30/2023	1.0	Language edits, and document formatting	CMS DPO ISSO
5/1/2023	1.0	Added language regarding appropriately assign MARx roles to plan employees (pg.3)	CMS DPO ISSO
5/2/2023	1.0	Added language regarding EPOCs submitting an SOP with their annual designation letter to DPO (pg. 7)	CMS DPO ISSO
05/08/2023	1.0	Answered questions from OIT in comments. Made edits to language on the MARx/IDM roles	CMS DPO ISSO
05/09/2023	1.0	Finished answering questions from OIT in comments regarding AC-05 security control	CMS DPO ISSO
05/16/2023	1.0	Finalized v1.0 for dissemination to EPOCs	CMS DPO ISSO

1 External Point of Contact (EPOC) Rules of Behavior

The Centers for Medicare & Medicaid Services (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. External Point of Contacts (EPOC) are employed representatives of a Medicare Advantage (MA) or Prescription Drug plan/sponsor (PDP) who's purpose is to manage and grant their company's employee access to the Medicare Advantage Prescription Drug System (MARx). All employee users granted access shall use Medicare beneficiary data for conducting Medicare business only.

Users should only use MARx data for the business of Medicare, such as preparing an accurate Medicare enrollment, determining eligibility for specific services, reconciling premium and premium withhold, and reconciling a calculated beneficiary level payment. CMS expects MA/PDP's authorized staff to use and disclose PHI according to the CMS regulations. The HIPAA Privacy Rule mandates the protection and privacy of all health information. This rule specifically defines the authorized uses and disclosures of "individually identifiable" health information. The HIPAA Privacy Rule also ensures protection for patients by limiting the ways that physicians, qualified non-physician practitioners, suppliers, hospitals and other provider covered entities can use a patient's personal medical information.

This document explains the EPOCs responsibility in obtaining, disseminating, and using beneficiaries' Medicare eligibility, enrollment, premium, premium withhold, and payment data. It further explains the expectations for using MARx. An EPOC must adhere to these Rules of Behavior in order to maintain or grant access to the system. If the EPOC should violate these rules of behavior and/or other CMS data privacy and security rules, it could result in loss of access and other penalties.

CMS monitors an individual's access and their inquiries. CMS may contact MA plans, PDPs, and/or Third Party Vendors, herein referred to as "Users", identified as having unacceptable behavior (e.g., high inquiry volume, high error rate, inappropriate use of submitted transactions, inappropriate access to sensitive beneficiary or plan-level information, using automated processes for sending large numbers of inquiry requests in a short period of time) to verify and/or address improper use of the system or, when appropriate, refer them for investigation.

Any questions regarding EPOC rules of behavior or their responsibilities should be directed to the MAPD Help Desk at 1-800-927-8069 or mapdhelp@cms.hhs.gov and DPOEPOCS@cms.hhs.gov.

1.1 Providing MARx Access: EPOC Responsibilities

EPOCs are required to adhere to CMS Acceptable Risks and Safeguards (ARS) 5.0, Information Systems Security and Privacy Policy, and the CMS Risk Management Handbook. For more information, these guidelines and policies can be found on CMS' Information Security and Privacy webpage:

https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity

CMS Acceptable Risks and Safeguards (ARS) 5.0
https://security.cms.gov/policy-guidance/cms-acceptable-risk-safeguards-ars

Information Systems Security and Privacy Policy
https://www.cms.gov/research-statistics-data-and-systems/cms-information-technology/informationsecurity/info-security-library-items/cms-information-systems-security-and-privacy-policy-is2p2

CMS Risk Management Handbook (CMS Information Security and Privacy Library)
https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library

As a designated EPOC employed by a MAO/PDP, responsibilities are as following:

- Per the October 6, 2022 HPMS letter titled "Designation of Identity Management (IDM) Plan User Approver/External Point of Contact (EPOC)", EPOCs are required to:
    - Submit an EPOC designation letter and access acknowledgement form to CMS: The plan must email an official company letter to CMS identifying and appointing the EPOC.
    - Complete the initial registration in the Identity Manager (IDM): CMS requires organizations select a qualified official as their EPOC, such as a manager, supervisor of Information Technology, or a Systems Security Officer. After providing the preliminary information to CMS, the EPOC utilizes IDM to assign themselves as the steward of the appropriate contract number(s) as part of completing the registration process.

  - Perform annual role certification for their company and their users: 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. EPOCs are required to review and certify their company's end users annually and submit a new EPOC Designation letter to CMS between October and December each year.

- The EPOC is required to establish a standard operating procedure (SOP) for maintaining plan user access under their authority and in accordance with CMS Security Policies. The EPOC must send a copy of the SOP with their annual designation letter to DPOEPOCS@cms.hhs.gov

- EPOCs are required to keep their accounts active and current, and failure to access the IDM system within a 60-day period will automatically disable their account due to an expired password. EPOCs that experience this situation are required to contact the MAPD Help Desk to have their password reset.

- Adhere to the CMS Acceptable Risks and Safeguards (ARS) 5.0 security policy for Access Control-05 (AC- 05) which 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. MA/PDP plans will maintain a separation of duty by designating an EPOC the capability to set permissions for their company's staff when accessing PII (Personally Identifiable Information) and PHI (Protected Health Information) from CMS systems.

- EPOCs will promptly inform the MAPD Help Desk (1-800-927-8069 or mapdhelp@cms.hhs.gov) and the DPO Information Systems Security Officer (DPOEPOCS@cms.hhs.gov) when a security incident regarding misuse of PII/PHI occurs involving using the MARx system.

- EPOCs must adhere to the security requirements for users of CMS computer systems and to the basic desktop security measures to ensure the security of Medicare beneficiary personal health information. You must not:
  - Disclose, lend, or otherwise transfer identification numbers and/or passwords.
  - Use CMS data files for private gain or to misrepresent yourself or CMS.
  - Browse or use CMS data files for unauthorized or illegal purposes.
  - Disclose CMS data that is not specifically authorized.

EPOCs who violate any of these security requirements could lose systems access privileges and/or face disciplinary/adverse action up to and including legal prosecution. Federal, State, and/or local laws may provide criminal penalties for any person illegally accessing or using a Government-owned or -operated computer system.

1.2 Authorized Roles to Access MARx

In conjunction with the intent to provide health care services and determine health statuses for a Medicare beneficiary, the EPOC is authorized to grant access, and approve/deny each employees role in CMS' MARx system. Each role is described and listed below. However, if an EPOC needs assistance with determining a user's appropriate role because there is of the lack of clarity between the role and the user's employment duties, please contact the MAPD Help Desk at 1-800-927-8069 or mapdhelp@cms.hhs.gov and do not grant access to a different role as a substitute.

- MA Submitter - The person/entity directly affiliated with a MA/MAPD who will be responsible for electronically exchanging MA/MAPD data relative to enrollment, premium, premium withhold, and payment. The user is only able to view information for periods during which the beneficiary is/was enrolled in their company's health plan. This role also includes access to a Gentran mailbox. The user must select the Report Access Type of Financial or Non-Financial.

- MA Representative - The person/entity directly affiliated with a MA/MAPD who will be responsible for only viewing data relative to enrollment, premium, premium withhold, and payment. The user is only able to view information for periods during which the beneficiary is/was enrolled in their company's health plan.

- MCO Representative UI Update - The person/entity directly affiliated with a MA/MAPD who will be responsible to view, manually key-in, and/or correct their health plans beneficiary enrollment related data through the MARx online user interface. The user is able to view only enrollment, premium, premium withhold, and payment information for periods during which the beneficiary is/was enrolled in their company's health plan.

- MCO POS Edit User - The person/entity directly affiliated with a Point of Sale (POS) Drug Edit company who will be responsible for viewing, manual key-in and/or correct their health plans beneficiary POS Drug enrollment related data through the MARx online user interface. The user cannot view enrollment, premium, premium withhold, or payment information.

- MMP User - The person/entity directly affiliated with a Medicare and Medicaid Plan (MMP) who will be responsible for only viewing data relative to enrollment, premium, premium withhold, and payment. The user is only able to view information for periods during which the beneficiary is/was enrolled in their company's health plan.

- PDP Representative - The person/entity directly affiliated with a Prescription Drug Plan (PDP) who will be responsible for only viewing data relative to enrollment, premium, premium withhold, and payment. The user is only able to view information for periods during which the beneficiary is/was enrolled in their company's health plan.

- PDP Submitter - The person/entity directly affiliated with a PDP who will be responsible for electronically exchanging PDP data relative to enrollment, premium, premium withhold, and payment. The user is only able to view information for periods during which the beneficiary is/was enrolled in their company's health plan. This role also includes access to a Gentran mailbox. The user must select the Report Access Type of Financial or Non-Financial.

- NET Representative - The person/entity directly affiliated with a LI-NET (Limited Income Newly Eligible Transition) company who will be responsible for only viewing data relative to enrollment, premium, premium withhold, and payment. The user is only able to view information for periods during which the beneficiary is/was enrolled in their company's health plan.

- NET Submitter - The person/entity directly affiliated with a LI-NET company who will be responsible for electronically exchanging data with CMS relative to enrollment, premium, premium withhold, and payment. The user is only able to view information for periods during which the beneficiary is/was enrolled in their company's health plan. This role also includes access to a Gentran mailbox. The user must select the Report Access Type of Financial or Non-Financial.

- POSFE Contractor - The person/entity directly affiliated with a Point-of-Sale Facilitated Enrollment (POSFE) contractor who will be responsible for viewing, manual key-in and/or correct their health plans beneficiary enrollment related data through the MARx online user interface. Point-of-Sale Facilitated Enrollment (POSFE) contractor cannot enter or select contracts in IDM when registration occurs. IDM will assign the contract number as 'R0000' once the user is approved.

- Report View - The person/entity directly affiliated with a MAO/PDP who will be responsible for submitting request to download MARx reports/data relative to enrollment, premium, premium withhold, and payment. The user is only able to request daily, weekly, monthly MARx reports their company's health plan. This role also includes access to a Gentran mailbox. The user must select the Report Access Type of Financial or Non-Financial.

- All roles, excluding the MCO POS Edit User and Report View, include a functionality to verify eligibility for the "entire" Medicare population by entering the beneficiary's Medicare Beneficiary Identifier (MBI) or the Social Security Number (SSN), to determine Medicare eligibility for Part A or Part B of Medicare.

1.3 Authorized Purposes for Accessing MARx

The following are examples of authorized purposes for requesting access to Medicare beneficiary information:

- Determine if Medicare is the primary or secondary payer.
- Determine if the beneficiary is in original Medicare, Medicare Advantage, or Prescription Drug.
- Determine Low-Income Subsidy (LIS) Status.
- Determine Number of Uncovered Months for Part D (Credible Coverage).
- Determine beneficiary statuses for the purpose of enrollment, premium, premium withhold, and payment reconciliation.
- View or submit transactions/information related to enrollment, premium, premium withhold, and payment.
- Request reports be distributed to the MA/PDP related to enrollment, premium, premium withhold, and payment.

1.4 Unauthorized Purposes for Accessing MARx

The following are examples of unauthorized purposes for requesting access to Medicare beneficiary information:

- To determine eligibility for Medicare without screening the patient to determine if they are Medicare eligible.
- To acquire the beneficiary's health insurance claim number (HICN).
- Any action that violates HHS Rules of Behavior and/or CMS Security Policies.

- Approving/Substituting access to any MARx role due to the lack of information displayed or the lack of availability within a role that's fits the user's employment duties.