



CENTERS FOR MEDICARE & MEDICAID SERVICES

DATE: February 23, 2024

TO: All Current and Prospective Medicare Advantage, Prescription Drug Plan, Section 1833 and 1876 Cost, PACE, and Demonstration Organizations

FROM: Vanessa S. Duran, Acting Director
Medicare Drug Benefit and C & D Data Group
Center for Medicare

Kathryn A. Coleman, Director
Medicare Drug & Health Plan Contract Administration Group
Center for Medicare

SUBJECT: Instructions for Requesting Plan Electronic Signature Access in the Health Plan Management System (HPMS)

CMS requires that authorized officials of the organization – specifically, the Chief Executive Officer (CEO), Chief Financial Officer (CFO), and/or Chief Operating Officer (COO) – sign documents and complete attestations using the electronic signature process in HPMS.

These signatures include, but are not limited to, the following:

- Contracts
- Addenda
- Benefit attestations
- Agent/broker compensation attestations
- Medical Loss Ratio attestations
- Program audits
- Submission of service area reductions
- Medication therapy management attestations
- Part D payment reconciliation attestations
- Risk adjustment certifications
- Certification of monthly enrollment and payment data

Eligibility for Electronic Signature Access

To be eligible for electronic signature access in HPMS, the prospective signatory must meet **all** the following criteria:

- Serve as a direct employee of organization (i.e., not in a consultant or contractor capacity).
- Serve officially as the organization’s CEO, CFO, or COO. These individuals must have been duly appointed by the organization’s board or other governing body. **This authority cannot be delegated to an individual outside of these official roles.**
- Be recorded in the HPMS Basic Contract Management Module (i.e., on the Contact Data page) in the corresponding role below:
 - CEO - CMS Administrator Contact
 - CEO - Senior Official for Contracting
 - Chief Financial Officer
 - Chief Operating Officer

An individual that fails to meet all the criteria noted above is ineligible for electronic signature access. **If CMS discovers that a signatory does not meet these criteria, documents signed and attestations completed by that signatory, including MA and Part D contracts, may be deemed invalid.**

Process for Requesting Electronic Signature Access

The table below provides customized instructions that correspond to distinct user scenarios:

User Scenario	User Access Instructions
<p>A new user that needs both a CMS user ID and electronic signature access in HPMS</p>	<p>Complete a request for a CMS user ID via EFI submission.</p> <p>Instructions are available at: https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/HPMS/UserIDProcess.html</p> <p>Users can also visit the YouTube video created for plan users accessing EFI at: https://youtu.be/LeLICfJZYg</p> <p>Complete the steps described in Attachment A to request electronic signature access.</p>

User Scenario	User Access Instructions
<p>An existing HPMS user that needs to add electronic signature access</p>	<p>Complete the steps described in Attachment A to request electronic signature access.</p>
<p>An existing HPMS electronic signature user that needs to add or delete contracts</p>	<p>Complete the steps described in Attachment A to request the addition or removal of contracts for electronic signature access.</p>
<p>An existing HPMS electronic signature user with no changes needed</p>	<p>Complete the system access certification (SAC) and security computer-based training (CBT) on an annual basis, and current access will be retained without further action. Review Attachment B for recertification and password guidance.</p>

In accordance with the HPMS Rules of Behavior, the sharing of CMS user IDs is **strictly prohibited**. If CMS determines that individuals are sharing a user ID, the user ID will be revoked immediately.

For questions related to this memo, please contact HPMSConsultantAccess@cms.hhs.gov.

Attachment A - Requesting Electronic Signature Access or to Add or Delete Contracts for Existing Electronic Signature Access

To add electronic signature access or to add or delete contracts for existing electronic signature access, the user must perform the following steps:

1. Prepare an official letter that states the user's name, role (i.e., CEO, CFO, or COO), CMS user ID, contract number(s), and that electronic signature access is required. The letter must be provided on the organization's official letterhead **and** signed by a senior official of the organization. Organizations can request electronic signature access for more than one signatory on a single letter. CMS recommends the use of the following sample language:

(Name of Organization) hereby requests that (Name of Individual, CEO/CFO/COO role, and CMS user ID) be granted electronic signature access for the following contract number(s): (list specific contract numbers).

2. Submit the official letter via e-mail in scanned PDF format to HPMSConsultantAccess@cms.hhs.gov. To facilitate timely processing, please indicate electronic signature access in the subject line of the e-mail.

Attachment B - Recertification and Password Maintenance

Annual Recertification Process

CMS user IDs must be recertified electronically on an annual basis using CMS' System Access Certification (SAC) application at <https://eua.cms.gov/eurekify/portal/login>. For assistance with the SAC, the security computer-based training (CBT), and passwords, please contact the **CMS IT Service Desk at 1-800-562-1963 or 410-786-2580**.

If you do not complete the recertification in a timely manner, your CMS user ID will be revoked, and you will have to re-apply as a new user.

Upon receipt of a recertification email notice from eua@cms.hhs.gov, you must complete both Steps 1 and 2:

Step 1: System Access Review

1. Log into the SAC at <https://eua.cms.gov/eurekify/portal/login> using your HPMS credentials.
2. If you find a certification item on your home screen, select the "Certify" button to proceed.
3. Select the check box that appears next to your name. This action will automatically select the check boxes for all associated job codes.
4. Select the "Keep" button to retain access to the selected job codes.
5. On the summary page, select the "Submit" button to continue.
6. On the confirmation pop-up window, select the "X" that appears in the upper right-hand corner to complete the system access review step.

Step 2: Security Training

1. Log onto the system at <https://www.cms.gov/cbt/login> using your four-character CMS EUA user ID and eight-character CMS EUA password.
2. Enter your CMS user name only into the CMS EUA user ID field. Type your password into the password field. Do not cut/copy and paste your password into the password field.
3. Set up your multi-factor authentication (MFA) preference for the CMS IDM. *Note: This process is different than the process for establishing MFA preferences for accessing HPMS.*
4. Agree to the Terms & Conditions and click on Sign In.
5. Select the **Information Systems Security and Privacy Awareness Training** link on your dashboard.

6. Once on the course page, click on "Launch ISSPA Course," then select "Enter" to begin the ISSPA training course.
7. Once you have completed the training, sign and upload the Rules of Behavior to the "Rules of Behavior Upload" on the course page.
8. Once you have uploaded the Rules of Behavior, you are required to complete a short post-course evaluation.
9. Once you have completed the evaluation, your status will be updated to completed, and you will have access to the certificate of completion.

For technical assistance with the CBT, please send an email to CBT@cms.hhs.gov.

Step 3: Checking Your Status

You can check your System Access Review (SAC) status and last completed CBT date in EUA at any time.

1. Log into EUA at <https://eua.cms.gov> using your HPMS credentials.
2. Click on the "View My Identity" button or use the link from the left-hand navigation bar under the "Home" header.
3. Your identity information will appear on the subsequent page.

Your SAC has been completed when the: (a) SAC Recert Status is "OK," (b) SAC Recert Completion Date has changed to the day you completed your system access review, and (c) SAC Recert Due Date changed to the following year.

Your SAC is pending CMS approval when the SAC Recert Status is "Pending."

Your SAC has not been completed when the SAC Recert Status is "Due."

The CBT Recert Due Date reflects the next date the CBT is due. The CBT Completion date should reflect the day you completed your CBT, while the CBT Recert Due Date should reflect the following year.

If your CBT is within 4 weeks of the due date, you must complete the security CBT as described in Step 2 above. Please note that your CBT date will be updated in 2-24 hours, not immediately. However, if the CBT date remains unchanged, send a screenshot of your CBT dashboard showing the check marks next to each of the steps to CBT@cms.hhs.gov and request that CMS update your CBT status manually in EUA.

For additional information, please visit: <https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/HPMS/RecertAndPwdProcess.html>.