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

CMS

CENTERS FOR MEDICARE & MEDICAID SERVICES

DATE: April 11, 2025

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

FROM: Vanessa S. Duran, 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

Jennifer Lazio, Director
Parts C & D Actuarial Group
Office of the Actuary

SUBJECT: Instructions for Requesting Consultant Access to the Health Plan Management System (HPMS)

This memo provides guidance to Medicare Advantage, Prescription Drug Plan, Section 1833 and 1876 Cost, PACE, and Demonstration organizations whose consultants may require access to HPMS to perform business functions on their behalf. CMS requires sponsoring organizations to submit official letters to authorize HPMS access for these designated consultant users.

The following table outlines the consultant user profiles that are currently supported by HPMS:

User Type	HPMS Functionality
Actuarial Certification Consultant (consultants or plan employees serving in this role)	This user completes the actuarial certification portion of the bid submission process. An actuarial consultant that is not a direct employee of the organization may perform this function on behalf of multiple sponsoring organizations. Plan employees serving in this role will only perform this function on behalf of their own organization.

User Type	HPMS Functionality
Bid Consultant	This user prepares and/or submits plan bids on behalf of an organization. The consultant is not a direct employee of the organization and may perform this function on behalf of multiple sponsoring organizations. The sponsoring plan organization must clearly state if the bid consultant user also requires the **PBP/BPT Final Submit** access type, which will allow the user to perform the final submission of the PBP/BPT data in HPMS. Note: To grant PBP/BPT final submission access to direct plan employees, the plan organization must send an email to the hpms_access@cms.hhs.gov mailbox requesting the assignment of the **PBP/BPT Final Submit** access type. This email must include the user name(s), CMS user ID(s), organization name, and contract number(s) for which PBP/BPT final submission access is needed.
Formulary Consultant	This user prepares and/or submits formulary and related data on behalf of an organization. The consultant is not a direct employee of the organization and may perform this function on behalf of multiple sponsoring organizations.
Marketing Consultant	This user prepares and/or submits marketing materials on behalf of an organization. The consultant is not a direct employee of the organization and may perform this function on behalf of multiple organizations. There are two access types for marketing consultants. The sponsoring plan organization must clearly identify which type of access is being requested in their authorization letter. **Multi-Plan Marketing Submitters:** This user prepares and/or submits marketing materials on behalf of multiple organizations using the multi-plan marketing material submission process. User access is limited to the multi-plan portion of the HPMS Marketing Module. **Standard Marketing Consultant:** This user prepares and/or submits marketing materials using the standard plan marketing material submission process, essentially as an authorized plan user.

User Type	HPMS Functionality
Plan Reporting Data Validation Consultant	This user submits plan reporting data validation findings via the Plan Reporting Data Validation Module. The consultant is not a direct employee of the organization and may perform this function on behalf of multiple sponsoring organizations.
General Consultant	This user prepares and/or submits various data on behalf of an organization. The consultant is not a direct employee of the organization and may perform similar functions on behalf of multiple sponsoring organizations. **Note**: This category is intended to capture functionality that resides outside of the other defined consultant types (e.g., application submission, audit support, and performance assessment monitoring). The sponsoring organization must identify the functions needed by each general consultant using the General Consultant User Access form available at: https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/HPMS/UserIDProcess.html

The consultant access instructions are determined by a given user's current access situation. The table below provides the submission requirements for each of the following user scenarios:

User Scenario	Submission Requirements
A new user that needs a CMS user ID *and* consultant access in HPMS	Complete a request for a CMS user ID via ICT (formerly known as EFI) making sure to select the correct consultant type for the question "I am a." Instructions can be found on https://www.cms.gov/Research-Statistics-Data-and-Systems/Computer-Data-and-Systems/HPMS/UserIDProcess.html under the Downloads section (Instructions for Requesting Plan Access via EFI). Users can also visit the YouTube video created for consultant users accessing ICT: https://youtu.be/KAXwdnq1hKs Complete the steps described in **Attachment A** to request consultant access. Include the completed General Consultant form in the submission, if applicable.
An existing HPMS user that needs to add consultant access	Complete the steps described in **Attachment A** to request consultant access. Include the completed General Consultant form in the submission, if applicable.

User Scenario	Submission Requirements
An existing HPMS consultant user that needs to add or delete contracts	Complete the steps described in **Attachment A** to request the addition or removal of contracts for consultant access. Include the completed General Consultant form in the submission, if applicable.
An existing HPMS consultant user with no changes needed	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.

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.

Managing HPMS User Access

Ultimately, it is the responsibility of the sponsoring organization to manage and maintain the set of users for whom they have authorized access to HPMS. This general principle applies to both plan staff and any consultants that are serving as agents of the sponsoring organization.

There are reports in HPMS that can be used to manage user access to their contract number(s). These reports can be viewed under the "User Resources > User Access Administration" link in HPMS. If a user within a sponsoring organization does not currently have access to the "plan user access" reports, organizations must submit an access request to hpms_access@cms.hhs.gov.

Sponsoring organizations may request to remove a user's HPMS access at any time. These requests should be sent to hpms_access@cms.hhs.gov. Requests must contain the user ID, the name of the individual, the individual's organization name, the proposed change, and the reason for the change.

In the case of consultant users, it is **critical** to remember that these individuals typically serve multiple organizations. When requesting the removal of a consultant, clearly state that the individual is a consultant and only request the removal of specific contract numbers, not the removal of the user's account. Failure to provide this level of detail may result in the deletion of a consultant's CMS user ID rather than simply the consultant's access to certain contract number(s).

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

Attachment A – Requesting HPMS Consultant Access or to Add or Delete Contracts for Existing Consultant Access

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

1. Prepare an official letter that states the user's name, CMS user ID, consultant company name, the type of consultant access being requested, and the contract number(s) for which consultant access is needed. The letter must be provided on the sponsoring organization's official letterhead **and** signed by a senior official of the organization. Organizations may submit one letter requesting access for multiple consultants, if the organization is requesting the same access type for all consultants listed. CMS recommends the use of the following sample language:

   (Name of organization) hereby requests that *(name of consultant user, the CMS user ID, and consultant company name)* be granted *(indicate type of consultant 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 the type of consultant access in the subject line of the e-mail.

   NOTE: If a user is serving multiple organizations, only **one** CMS user access form is required. However, an official letter must be provided from **each** organization for which the user will be serving as an agent in HPMS.

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.